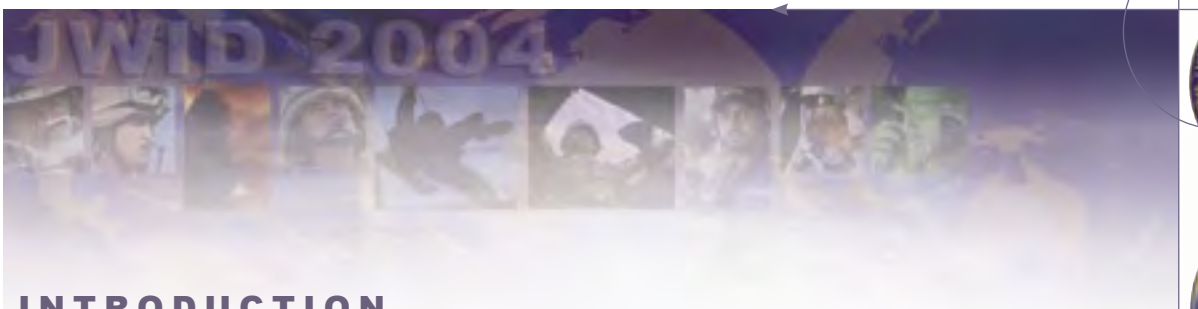


INTRODUCTION

Executive Summary

The Joint Warrior Interoperability Demonstration is an annual Chairman of the Joint Chiefs of Staff event with the international community to investigate command and control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) solutions to near-term coalition challenges. This year's event also investigated interoperability solutions with non-DoD agencies, including the Department of Homeland Security (DHS).

JWID provides the opportunity for information sharing among many entities, including homeland security and homeland defense partners, Department of Defense agencies, private industry, and coalition partners. Participants examine new and emerging C4ISR technologies and explore solutions to interoperability challenges in a multi-domain environment.

U.S. Northern Command (USNORTHCOM) was the host combatant commander and the Defense Information Systems Agency (DISA) was lead. In a departure from previous JWIDs, USNORTHCOM invited agencies within the Department of Homeland Security, including the Federal Emergency Management Agency (FEMA), the Federal Bureau of Investigation (FBI), the U.S. Coast Guard, and the National Guard Bureau to participate for the first time. U.S. Joint Forces Command filled an ancillary role, assisting with select fielding of technologies to combatant commanders.

This year's homeland security focus, along with continuing emphasis on coalition interoperability, made JWID 2004 an unprecedented challenge in the history of the program. USNORTHCOM expanded the definition of "coalition" to include inter-agency homeland security partners as well as allied militaries. This created broad opportunities to explore interoperability issues, but also created greater levels of complexity. Limited resources were stretched to meet the needs of both the "home game," the homeland security/homeland defense (HLS/HLD) mission, and the "away game," the traditional military coalition mission.

Challenges included adapting the program to meet civil objectives, improving the trial selection process, developing higher standards for trial submission, and creating a JWID execution environment reflective of the operational world.

2004 OBJECTIVES

1. Provide solutions to facilitate **information sharing across multiple information domains** that include defense and other government agencies. (Information Sharing/Multi-Level Security)

2. Provide an enhanced **interoperable situational awareness** capability, scalable in both time and scope within and between information domains. (Situational Awareness)

3. Provide enhanced methods to **fuse and protect information contained in dissimilar databases** maintained by coalition and national defense and government agencies. (Database Fusion)

4. Provide solutions to permit enhanced **sharing/dissemination of intelligence, surveillance, and reconnaissance (ISR) products** within and across coalition and inter-agency information domains. (ISR Dissemination)

5. Provide solutions to address **in-transit security of information** being shared within and between fixed information environments and mobile/tactical users. (Wireless Security)

6. Provide solutions to **monitor and defend against threats** to multiple information domains. (Coalition Network Defense)

7. Provide solutions to create a **fused logistical status** including information feeds from multiple information domains. (Logistics Systems)

8. Provide **language translation tools** to enable effective coalition and inter-agency operations. (Language Translation)

EVOLUTION

Transformation Change Package Candidates

Of top performers listed on the next page, nine trials stood out as potential warfighter capabilities to field within the next 12 to 18 months. Trials in the table below, in order of trial number, have been nominated to the Transformation Change Package (TCP) process:

POTENTIAL TCP CANDIDATES

UST01.09	Voltage Corp. Identity Based Encryption (VIBE)
UST01.10	Multi-Role Boundary Control ISSE
UST01.12	Mission Assurance Decision Support Capability Suite (MADS/CS)
UST02.07	Total Domain Server
UST02.09	Area Security Operations Command and Control (ASOCC)
UST06.03	NetScout
CIT01.05	PKI Express
CIT01.10	NetTop
CIT01.20	Secure Network Server (SNS)

SUCCESS STORIES

Trials are in transition to operational use after success during JWID 2004. Trials listed below have been, or are scheduled for, fielding. Operational use has exposed JWID technolgy to a broad audience of Federal Government and Department of Homeland Security officials.

UST01.12 Mission Assurance Decision Support Capability Suite (MADS/CS)

- Fielded by USNORTHCOM in conjunction with ASOCC, HLD COP, SWARM and JPEN trials.

UST01.13 Secure Wide Area Response Management (SWARM)

- Fielded by USNORTHCOM in conjunction with ASOCC, HLD COP, DMIS and JPEN trials.

UST01.14 Disaster Management Interoperability Service (DMIS)

- Proposed joint standard for the Department of Defense

UST01.15 Business Continuity Planning Virtual Command Center (BCP VCC)

- Fills requirements for several functions, including locating Marines in the National Capital Region. Cuts the process from days to hours. Will be fielded in the near future.

UST02.02 Rapid Response System (RSS)

- Used in disaster response to Hurricanes Charlie, Francis, and Ivan. Will be used during the Presidential Inauguration, and Marine Corps Marathon. Additional systems being purchased.

UST02.06 Joint Protection Enterprise Network (JPEN)

- 40 USNORTHCOM sites presently using prototype and will be integrated into JFHQ-NCR.

UST02.09 Area Security Operations Command and Control (ASOCC)

- Fielded by USNORTHCOM and the U.S. Marine Corps in support of Homeland Security.

UST02.16 Homeland Defense Common Operational Picture Support (HLD-COP)

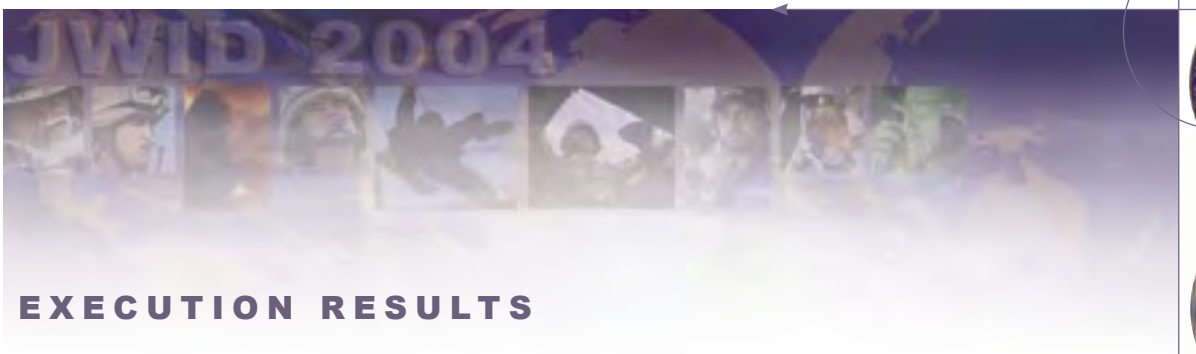
- Fielded at USNORTHCOMM DWC

UST05.02 Geospatial Intelligence Secure Wireless Advanced Imagery Dissemination

- Used during the Democratic and Republican National Conventions, deployed to both Korea and Iraq. Highly successful at the Democratic and Republican National Conventions and recognized for its potential use during the upcoming Presidential Inauguration.

CIT04.09 Enterprise Knowedge Management (eKM)

- Limited fielding under the U.S. Navy



EXECUTION RESULTS

Top Performers

The following list provides top performers from JWID 2004 based on assessment results and inputs from U.S. Northern Command (USNORTHCOM), U.S. Joint Forces Command (USJFCOM) and JWID Joint Management Office (JMO) working group staffs.

NOTE: The trials are listed in order of their trial number. No attempt is made to place one trial over the other in this list since they span several different objective areas and cannot be readily compared.

TRIAL NO.	TITLE (ACRONYM)	SPONSOR
UST01.09	Voltage Corp. Identity Based Encryption (VIBE)	DARPA/National Center
UST01.10	Multi-Role Boundary Control - Information Server Support Environment (MRBC-ISSE)	DARPA/ USNORTHCOM
UST01.12	Mission Assurance Decision Support Capability Suite (MADS/CS)	USNORTHCOM
UST01.13	Secure Wide Area Response Management (SWARM)	USNORTHCOM
UST01.14	Disaster Management Interoperability Service (DMIS)	US Marine Corps
UST02.06	Joint Protection Enterprise Network (JPEN)	Joint Staff/ USNORTHCOM
UST02.07	Total Domain	USNORTHCOM
UST02.09	Area Security Operations Command and Control (ASOCC)	USNORTHCOM
UST02.12	Regional Information Joint Awareness Network (RIJAN)	US Army
UST02.16	Homeland Defense Common Operational Picture Support (HLD-COP)	USNORTHCOM
UST06.02	Suite of Operationally Inexpensive Security Hosts (SOISH)	DARPA
UST06.03	NetScout Performance Manager 2.0 (NETSCOUT)	DISA
CIT01.01	Interactive Link	DISA
CIT01.05	PKI Express & Interop Express	DISA
CIT01.10	NetTop	NSA
CIT01.20	Secure Network Server (SNS)	USNORTHCOM
CIT02.17	Topspin	SPAWAR
CIT03.04	Coalition Blue Force Situational Awareness (CBFSA)	USSTRATCOM
CIT04.02	Satellite Coalition Broadcast Environment (SCoBE)	US Air Force
CIT04.09	Enterprise Knowledge Management (eKM)	US Navy

For brief descriptive text on top performers (and all trials), locate them through trial contents pages in this booklet:

USTS .....PG. 11

CITS .....PG. 25

Unabridged reports on all trials are available on a companion compact disc, or go to www.cwid.js.mil.

HISTORY

Today's JWID, more than 10 years of evolution

JWID traces its history to establishment of the Secure Tactical Data Network (STDN) series originated by the U.S. Army to demonstrate emerging command, control, communications and computer (C4) capabilities. STDN 1 and 2 concentrated on Army-only issues. STDN 3 brought the first multi-service participation.

The Joint Staff recognized that advances in communications and information technology in the public sector were outpacing Department of Defense capabilities. In 1993, they sponsored the STDN series under the C4I for the Warrior concept. Using the Defense Information Systems Agency (DISA) as the Executive Agent, the Joint Staff directed DISA, in concert with a lead Service, to organize network experiments to bring emerging public sector and other government agency technologies into DOD projects and into the warfighters' sphere of recognition, while improving joint C4 interoperability.

In 1994, STDN efforts evolved into the first JWID. The Air Force was the lead service and U.S. Atlantic Command (now U.S. Joint Forces Command) was the host combatant command. The idea of moving from a static, one-dimensional picture of the battlefield to a near real-time, multi-dimensional battlespace picture became reality. Key efforts in 1994 included demonstration of baseline segments of what became the Global Command and Control System (GCCS). Six weeks after the conclusion of JWID 1994, GCCS was operationally deployed to U.S. Atlantic Command to support military operations in Haiti. GCCS was fully deployed to all combatant commanders within 12 months.

In 1997, the Chairman of the Joint Chiefs of Staff mandated interoperability in Joint Vision 2010, envisioning future conflicts as coalition operations. JWID established itself as a coalition interoperability forum, inviting the Combined Communications Electronics Board (CCEB) nations (Australia, Canada, New Zealand and the United Kingdom) and NATO that year and continued to invite them every year since. While participants use JWID to perform their own technology demonstrations and joint interoperability trials, their main intent is to promote and ensure C4 interoperability with the U.S.

EXPANSION

In 1998, JWID evolved into a two-year process to pursue selection and limited fielding of C4 technologies to the warfighting combatant commanders. The Theme (first) Year conducted demonstrations and interoperability trials and selected "Gold Nuggets" for support and continued improvement during the Exploitation (second) Year. JWID 1998 fielded three Gold Nuggets selected from the results of 1997's demonstration.

Due to U.S. Y2K concerns, JWID 1999-R was revised to focus on coalition interoperability

trials between the U.S. and CCEB/NATO nations. To more easily promote such trials and other C4I experiments, the Combined Wide Area Network (CWAN) established annually for JWID evolved into the standing Combined Federated Battle Laboratories Network (CFBLNet). This important evolution now permits C4I experimentation among the U.S. and the nations of the CCEB/NATO on a year-round basis using a network jointly owned and managed by CFBL membership.

JWID 2000-2001 restored the two-year cycle, with 23 U.S. demonstrations and 145 combined/coalition demonstrations at multiple, worldwide sites. Two Gold Nuggets were fielded in 2001. In addition, a Distributed Collaborative Tool Set (DCTS, now Defense Collaboration Tool Suite) for CWANs was refined and subsequently selected for worldwide fielding to the Unified Commands. The JWID 2001 DCTS trial experience permitted DISA to field the capability, within 72 hours, in support of Office of the Secretary of Defense requirements following the terrorist attacks of September 11th, to multiple DOD networks.

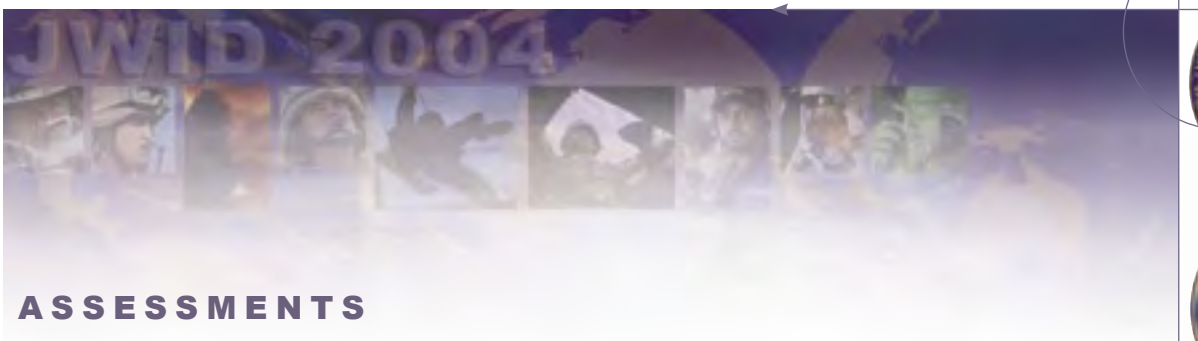
COALITION INTEROPERABILITY

JWID 2002 featured transition from a limited fielding of technology to a full focus on coalition interoperability, hosted by U.S. Pacific Command (USPACOM). The demonstration included Pacific Rim nations in a Pacific Theater Initiative (PTI), with Japan, South Korea, Singapore, and Thailand participating while Malaysia and the Philippines observed operations. Multiple coalition partners were integrated on the Multinational Task Force (MTF) and component staffs to maximize opportunities. In addition, the JWID CWAN continued use of CFBLNet architecture and services established in past demonstrations. U.S. Joint Forces Command (USJFCOM) fielded a JWID demonstrated language translation device following JWID 2002.

JWID 2003 took coalition interoperability to new heights. USPACOM guided the CTF and, for the first time, Japan, South Korea, Thailand and Singapore provided staffing to expand information exchange over dual domains. One key focus for 2003 was management of information exchange among the traditional "6-eyes" network to a larger, more robust "10-eyes" network. The larger network was vital to JWID's success because Pacific Rim nations needed effective information to serve in MTF staff positions. This offered an opportunity to address Information sharing/multi-level security technical solutions and refinement of coalition policies and procedures to overcome issues surrounding information exchange. Another milestone featured the Defense Information Systems Agency (DISA) assuming duties as the lead agency, providing broad-base management support to JWID activities. Four Coalition Interoperability Trials (CITs), with especially noteworthy performance, were submitted to USJFCOM for consideration for limited fielding as part of the new J861 Transformation Change Package (TCP) fielding process.

JWID 2004 welcomed U.S. Northern Command (USNORTHCOM) as the host combatant command through CWID 2005. USNORTHCOM brought a homeland defense (HLD) and Military Assistance to Civil Authorities (MACA) focus to the demonstration. This approach broke new ground beyond the traditional JWID coalition interoperability arena, adding government inter-agency information sharing. Though a number of technology demonstrations were applicable to the Homeland Security/Defense (HLS/HLD) community, JWID 2004 continued to predominantly address interoperability issues critical to the overseas combatant commanders – the "away game."

JWID 2004 involved 25 countries, military services and government agencies participating in a scripted scenario over a global network.



ASSESSMENTS

Focus on Solutions

By introducing U.S. Northern Command as the host combatant command, JWID 2004 attempted to realign a traditional military-centric venue to also address post-9/11 security concerns. Traditional Joint and Coalition C4I technologies supporting military warfighters were accompanied by technologies that supported government agencies on the national and local level.

The Technical Assessment Security and Warfighter Evaluation Working Group (TASWEWG) provides the Joint Staff, Combatant Commanders and other interested parties with an objective assessment of each qualifying Coalition Interoperability Trial (CIT) or U.S. Interoperability Trial (UST).

The ultimate goal of the assessment effort was to determine how well the trials provided solutions or enhancements to C4 interoperability challenges facing Joint, Coalition, Homeland Security and Homeland Defense operations.

The TASWEWG organization is three teams of analysts: Warfighter/Operator Utility, Interoperability and Security. These analyst teams were supported by representatives from the JWID Joint Management Office (JMO), Joint Interoperability Test Command (JITC), National Security Agency (NSA) and Coalition nations. The analyst teams scrutinized each trial to determine the level of assessment to be performed, collected data prior to and during execution to support a comprehensive assessment and prepared this final report at the conclusion of execution.

JWID 2004 built on previous years efforts to increase coalition participation in the assessment process. Coalition nations were fully integrated into the TASWEWG and, like their U.S. counterparts, were responsible for assessment planning/preparation, data collection and reporting functions for their own nations sponsored trials as well as data collection for all trials participating from their respective nation's sites during JWID execution.

The enhanced cooperation across all U.S. and coalition assessment activities increased the validity of the assessment process and provided the additional rigor required to carry forward JWIDs promising technologies to the operational environment.

WARFIGHTER/OPERATOR UTILITY ASSESSMENT

The warfighter/operator assessment focused on the trial's "value added" to the warfighter/operator, its technical performance and the ability to meet stated objectives and capabilities in

support of the JWID objectives in an operational environment.

During JWID execution, warfighters/operators and staff personnel operated and interacted with the trials and evaluated the system's utility by completing JWID network accessible questionnaires generated via Joint Battle Center (JBC) Data Collection and Analysis Tool (JDCAT). The questionnaires were specifically developed for each trial based on the following criteria:

- Objectives mapped back to the JWID objectives
- Predefined Master Scenario Events List (MSEL) events and/or definitive test schedules
- Trial capabilities
- Applicable Measures of Performance (MOPs) tailored to each trial

INTEROPERABILITY ASSESSMENT PROCESS

Throughout the planning/preparation cycle, JITC worked with each trial to define system interfaces to be exercised during JWID execution. For those trials that lacked formal requirements documentation, JITC worked with trial staff experts to write Information Exchange Requirements (IERs) defining data characteristics associated with each interface. The IERs defined who exchanges information with whom, what information is exchanged, how the information is exchanged, why the exchange is necessary and how the exchange takes place.

During JWID execution, JITC witnessed data exchanges between systems to ensure that the data transferred was received and processed correctly by the receiving system. All information collected by JITC can be applied to any future formal U.S. interoperability certification process, leading to faster fielding of products demonstrated during JWID.

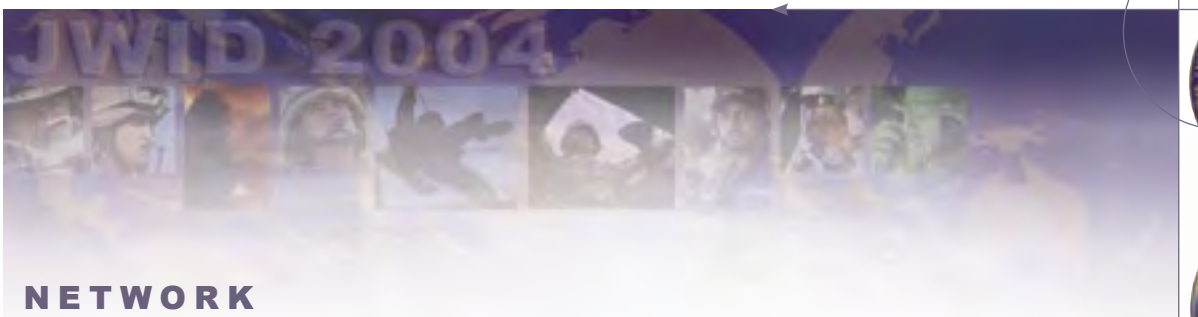
SECURITY ASSESSMENT PROCESS

The security assessment focused on how the trial countered identified threats and enforced identified policies consistent with appropriate usage assumptions for the projected warfighting environment. The Security Environment Elements are threats, assumptions and policies which a system or product might affect within that environment. Each assessed trial was documented for ability to counter environmental threats and enforce environmental policies consistent with its intended use. Threats and policies that were adequately addressed by the capabilities of the trial were identified as "security coverage." Threats and policies not adequately addressed by the trial were a "security exposure." Security exposures that could be addressed by other elements represented "residual risks" that must be managed for a successful deployment.

JWID EXECUTION

During JWID execution, TASWEWG members were present at and collected assessment data from five U.S. sites as well as coalition sites in Australia, Canada, NATO, New Zealand and the United Kingdom.

Sixty-one trials participated in JWID 2004, of which the TASWEWG formally assessed 25 of 26 USTs and 29 of 35 CITs. The trials received various levels of assessment from the three-pronged warfighter/operator, interoperability and security assessment process. The Systems Engineering and Integration Working Group (SEIWG) reported on the remaining seven trials that were not formally assessed by the TASWEWG.



NETWORK

Connecting the Globe

U.S. Northern Command (USNORTHCOM), as the host command, used three major network domains to execute JWID 2004.

HIGH-LEVEL NETWORK TOPOLOGY

The three domains were named Combined Federated Battle Laboratories Network (CFBLNet) Warfighter Domain, Military Assistance to Civil Authorities (MACA) Domain, and National Domains. The CFBLNet represented the traditional JWID network of Allied nations of the Combined Coalition Electronics Board (CCEB), Australia, Canada, New Zealand, United Kingdom, and U.S. plus NATO (AUSCANNZUKUS plus NATO). The MACA Domain represented the network for homeland security/homeland defense, while the National Domains represented "secret" individual networks for Australia, Canada, United Kingdom and the United States.

CFBL NETWORK INFRASTRUCTURE

The CFBLNet was successfully implemented to support JWID. Designed as a secret-releasable overlay on the Defense Information Systems Network-Leading Edge Services (DISN-LES) and DISA ATM Services - Unclassified (DATMS-U) ATM backbone networks, the CFBLNet incorporated a sophisticated ATM backbone, capable of supporting high-speed data transmission requirements of up to 45 Mbps (million bits per second). In the U.S., the CFBLNet shared between 3 and 6 Mbps of bandwidth on the DISN-LES with U.S. National and MACA domains.

For JWID 2004 the CFBLNet consisted of 35 sites, connected with a sophisticated network of ATM transmission paths providing between 3-10 Mbps of bandwidth for data requirements. Throughout the exercise, the overall CFBLNet availability was 99.9998 percent based on Internet Protocol (IP) connectivity during the JWID day (1500 to 2100 Z) to each site.

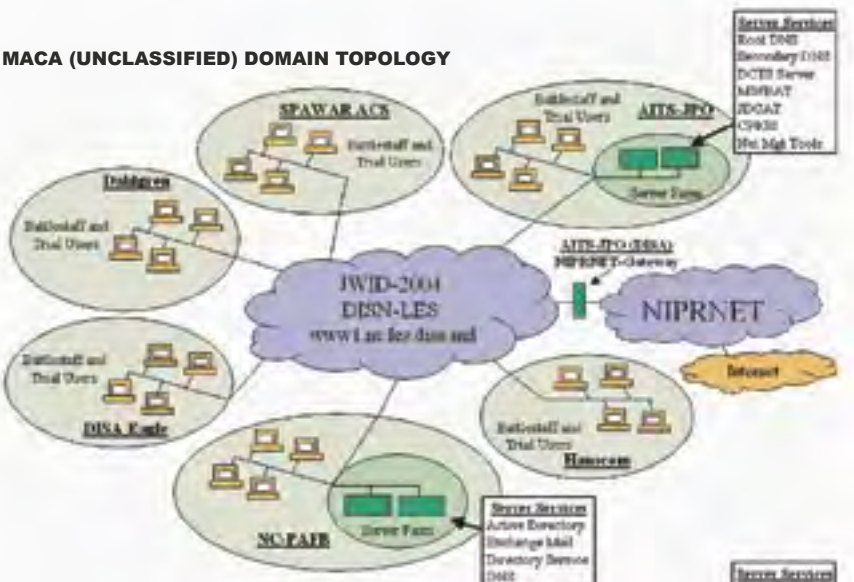
JWID 2004 involved the Republic of Korea (ROK) a non-traditional coalition ally. As a result, three additional domains were implemented in connection with the CFBLNet: the ROK domain; the NATO-Only domain; and the Partners for Peace (PfP) domain. The three information domains had to be created to ensure due diligence in protecting sensitive information as it passed between information domains. The three domains were organized into two classification levels termed "6-Eyes" and "8-Eyes." The 6-Eyes domain contained traditional allied nations of the CCEB. The 8-Eyes domain consisted of CCEB plus ROK and NATO). The CFBLNet for JWID 2004 facilitated additional NATO site participation through Allied backside connections. Many of these sites were connected to and participated on the CFBLNet with extensive local infrastructure. DISA's Advanced Information Technology Services-Joint Program Office (AITS-JPO) established and supported the traditional 6 Eyes and the ROK Domains.

CFBL NETWORK SERVICES

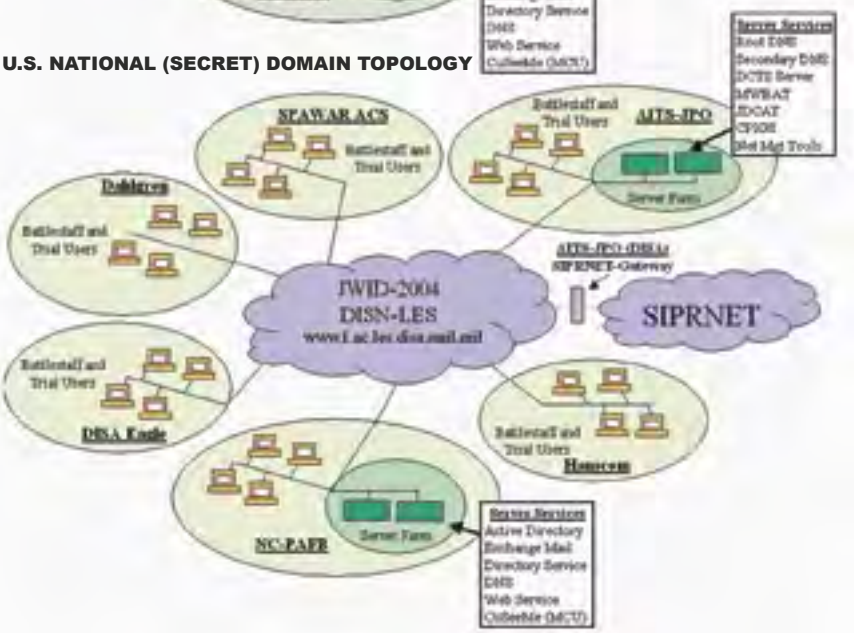
A coalition staff representing Australia, Canada, New Zealand, U.K., U.S. and NATO developed, planned, engineered, implemented and maintained CFBL network services for JWID 2004. The tasks required skills in UNIX and Windows platforms, network management tools, collaboration tools, web, Domain Name Service (DNS), and electronic mail (e-mail). The network services requirements for JWID this year were extremely complex, given the establishment of multiple coalition domains.

In addition to the traditional CFBLNet, the three additional domains required individual sets of core services. NATO stood up and provided core services to support the NATO-Only and PfP domains which were implemented on the national side of the NATO CFBLNet point of presence. The ROK domain was executed on the national side of the U.S. CFBLNet domain and was supported by a DII Mail guard and a Radiant Mercury guard which allowed filtered e-mail with attachments and the Common Operational Picture (COP) to flow between the AUSCANNZUKUS plus NATO and ROK domains.

MACA (UNCLASSIFIED) DOMAIN TOPOLOGY



U.S. NATIONAL (SECRET) DOMAIN TOPOLOGY



MACA AND U.S. NATIONAL NETWORKS

The MACA network was designed as an unclassified overlay on the DISN-LES and DATMS-U ATM backbone networks, while the U.S. National network was designed as a U.S. Secret overlay on the same backbone networks. The ATM backbone networks were capable of supporting high-speed data transmission up to 45 Mbps, however, only 3-6 Mbps of bandwidth was used for each site. This limited bandwidth was then shared among U.S. National, MACA, and CFBLNet.

Throughout the demonstration, overall MACA and U.S. National network availability was 100 percent based on IP connectivity during the JWID day to each site. Although sporadic network outages occurred during the JWID 2004 execution period, none affected the JWID day. During JWID 2004, traffic transmitted between sites was typically 2.5-3.5 Mbps, peaking above 6 Mbps throughout the JWID day.

NETWORK SERVICES

During JWID 2004, USNORTHCOM faced the dual challenge of not only participating in JWID 2004 as the Host Combatant Command for the first time, but also hosting the services on the MACA and U.S. National networks. USNORTHCOM was successful providing services as required, paving the way for a smooth execution period.

JWID PERSPECTIVES

Evolution of the program

U.S. AIR FORCE LEADS

1994 with U.S. Atlantic Command as host combatant commander:

- From static one-dimesional battlefield picture to near real-time, multi-dimensional battlespace picture
- Common Operational Picture (COP)
- All Source Tracking System
- Tactical Packet Networks
- Asynchronous Transfer Mode (ATM)
- Information sharing/multi-level security (MLS) + Server

U.S. MARINE CORPS LEADS

1995 with U.S. Pacific Command as host combatant commander:

- Collaborative Contingency Targeting
- Contingency Theater Automated Planning System
- Global Broadcasting System (GBS)
- Theater Deployable Communications
- Information sharing/multi-level security (MLS) + Server

U.S. ARMY LEADS

1996 with U.S. Central Command as host combatant commander:

- Joint Total Asset Visibility
- Common Operational Modeling, Planning, and Simulation Strategy (COMPASS)
- Global Command and Control System (GCCS)
- Common Operational Picture (COP) validation

U.S. NAVY LEADS

1997-1998 with U.S. Atlantic Command as host combatant commander:

- Interoperability mandated in Joint Vision 2010
- Invited Combined Communications Electronics Board (CCEB) nations (Australia, Canada, New Zealand, United Kingdom)
- Common Operational Modeling, Planning, and Simulation Strategy (COMPASS)
- Increased Compression Engine (ICE)

1994

1995, 2002

1996

1997-1998

1999, 2000-2001

2003

- Radiant Mercury Imagery Guard

U.S. AIR FORCE LEADS

1999-Revised with U.S. Joint Forces Command as host combatant commander:

- U.S. Y2K concerns drove revision to exclusive CCEB nations and NATO network support
- Combined Wide Area Network (CWAN) transition to Combined Federated Battle Laboratories Network (CFBLNet)
- COP Interface eXchange
- eXtensible Markup Language (XML) viewing of Air Tasking Order (ATO)

U.S. AIR FORCE LEADS

2000-2001 with U.S. Space Command as host combatant commander:

- Silent Runner® and PATROL© Gold Nuggets fielded
- Emphasis on Coalition Interoperability Trials (CITs)
- Support from National Imagery and Mapping Agency (NIMA, now NGA)
- Defense Messaging System (DMS)
- GCCS first COP exchange with Allied networks

U.S. MARINE CORPS LEADS

2002 with U.S. Pacific Command as host combatant commander:

- Inclusion of Pacific Rim nations in Pacific Theater Initiative (PTI)
- Comprehensive assessment methodology
- Language translation services in an instant messaging format

DEFENSE INFORMATION SYSTEMS AGENCY (DISA) LEADS

2003 with U.S. Pacific Command as host combatant commander:

- Dual domain network characterized as “6 eyes” and “10 eyes” to describe security access groups
- Core services led/supported by coalition nations
- Four Coalition Interoperability Trials advanced to U.S. Joint Forces Command for fielding to combatant commanders

UST CONTENTS

U.S. Assessment Briefs

U.S. INTEROPERABILITY TRIALS

Peterson AFB, Colo.
DISA Eagle, Va.
Dahlgren, Va.
SPAWAR, Calif.
Hanscom AFB, Mass.

ACRONYMS AND ABBREVIATIONS

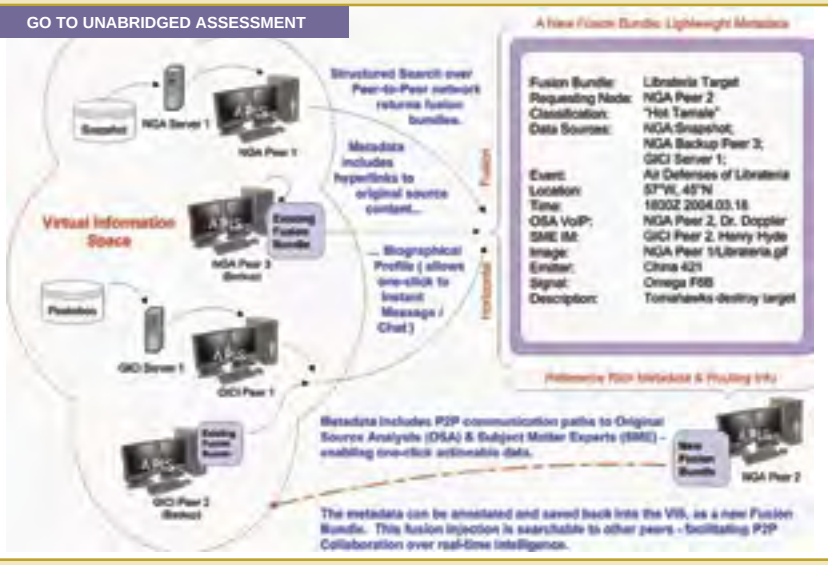
The reference list for the entire report is on the inside back cover of this booklet.

UST01.01

Advanced Peer Information Sharing

APIS leveraged Peer-to-Peer (P2P) networking with Structured Search technology to discover information across operational workspaces and established a net-centric Virtual Information Space (VIS) which returned actionable data as well as advanced dynamic warfighting capabilities. Analysts shared directories across a P2P network and published documents while searching their peer's real-time work flows. Queries returned metadata with hyperlinks to original source content, Subject Matter Expert biographies and one-click Instant Message collaboration.

GO TO UNABRIDGED ASSESSMENT



SPONSOR: NGA, CAN
TRIAL LOCATION: NSWC Dahlgren; NGA; Canada
TRIAL PARTNERS: N/A
OBJECTIVES: Information sharing/multi-level security, situational awareness, database fusion and ISR dissemination

ASSESSMENT RESULTS: During JWID 2004, APIS received a warfighter and interoperability assessment.

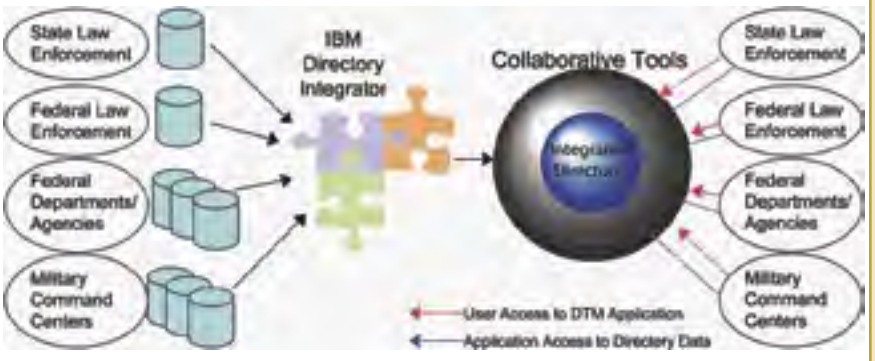
- APIS successfully met stated JWID objectives while collaborating and annotating geospatial images and map data between Canada and NGA.
- Geo and image analyst warfighters collaborated through images and maps and annotated them using an internal markup software which then provided staff personnel with valuable decision making information.
- Provided accurate intelligence analysis synthesized from multiple sources to warfighters that required the data without creating information overload.

UST01.02

Dynamic Team Management

DTM was developed to support organizations participating in Homeland Security/Defense Command and Control (HLS/D C2) Advanced Concept Technology Demonstration (ACTD). DTM provided planners the ability to integrate and leverage directory information across organizations, driven by the needs of emerging situations. DTM addressed building the best teams for each mission/task or accommodating information sharing preferences of participating organizations, directory integration automation, and dynamic scaling.

GO TO UNABRIDGED ASSESSMENT



SPONSOR: USNORTHCOM
TRIAL LOCATION: USNORTHCOM; DISA Eagle; NSWC Dahlgren; ESC Hanscom
TRIAL PARTNERS: UST01.13, UST02.09
OBJECTIVES: Information sharing/multi-level security, situational awareness and database fusion

ASSESSMENT RESULTS: During JWID 2004, DTM received a warfighter and interoperability assessment.

- DTM successfully met stated JWID objectives by integrating multiple organizational directories from conceptually different data storage schemas for team collaboration in themed workspaces that supported specific missions.
- Most warfighters indicated DTM was a effective collaboration and search tool and that its integrated directory between agencies was extremely useful.

UST01.03

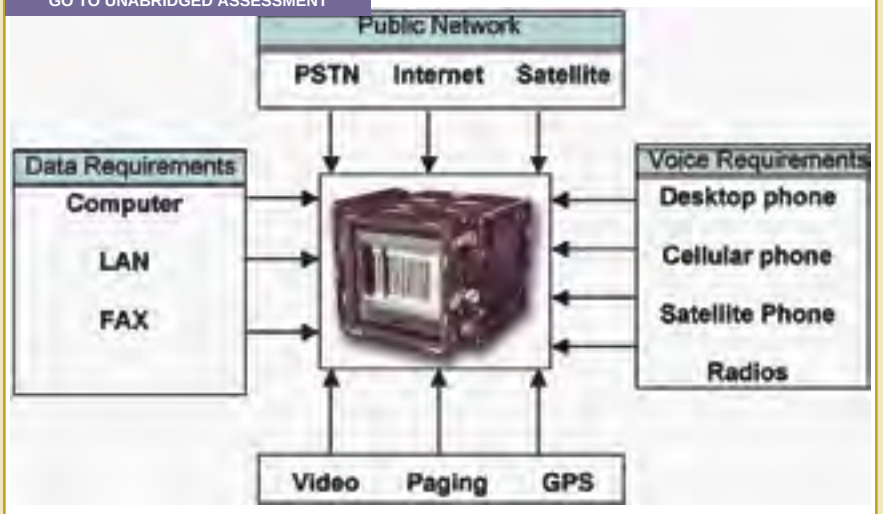
ReadySET

ReadySET was designed as an interoperable suite of communications modules engineered to provide flexible, scalable, upgradeable and deployable communications capabilities.

SPONSOR: USNORTHCOM, NGB
TRIAL LOCATION: NSWC Dahlgren
TRIAL PARTNERS: UST03.03
OBJECTIVES: Information sharing/multi-level security, situational awareness, ISR dissemination and wireless security

ASSESSMENT RESULTS: During JWID 2004, ReadySet received a warfighter and interoperability assessment

GO TO UNABRIDGED ASSESSMENT



- ReadySET successfully demonstrated stated JWID objectives by providing an interface to public and private networks, allowing interoperability between radio and wire-line devices, while integrating telephone, digital imagery, data and two-way radio.
- Warfighters unanimously agreed that ReadySET could be easily integrated, was transportable and provided effective communications between simulated first-responders and the Joint Operations Center.

UST01.08

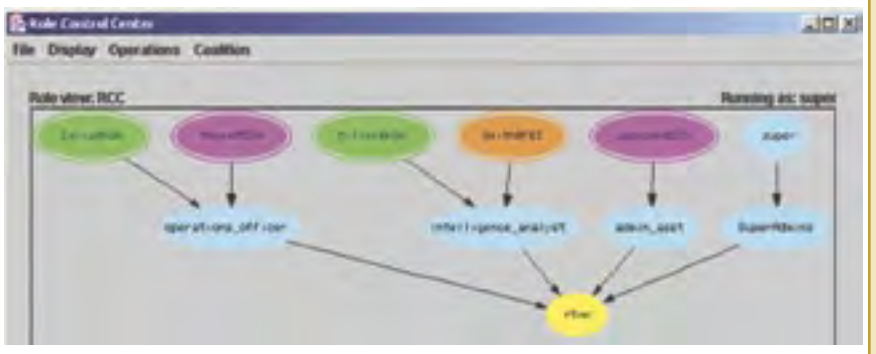
Multi-Domain Role Control Center

MDRC2 implemented role-based access control methods and tools for rapid formation of secure, dynamic coalitions and interagency information sharing environments. Roles were established to define authorization sets to access, grant or revoke individual access to information resources. The MDRC2 product was designed to enable dynamic coalition/interagency group formation while reducing set-up time from weeks to a matter of hours. MDRC2 supported joint administration access to coalition-critical resources without reliance on a single point of trust.

SPONSOR: DARPA, USNORTHCOM
TRIAL LOCATION: USNORTHCOM
TRIAL PARTNERS: UST01.09, UST01.10, UST06.02
OBJECTIVES: Information sharing/multi-level security and ISR dissemination

ASSESSMENT RESULTS: During JWID 2004, MDCRC2 received a security assessment and SEIWG evaluation report.

GO TO UNABRIDGED ASSESSMENT



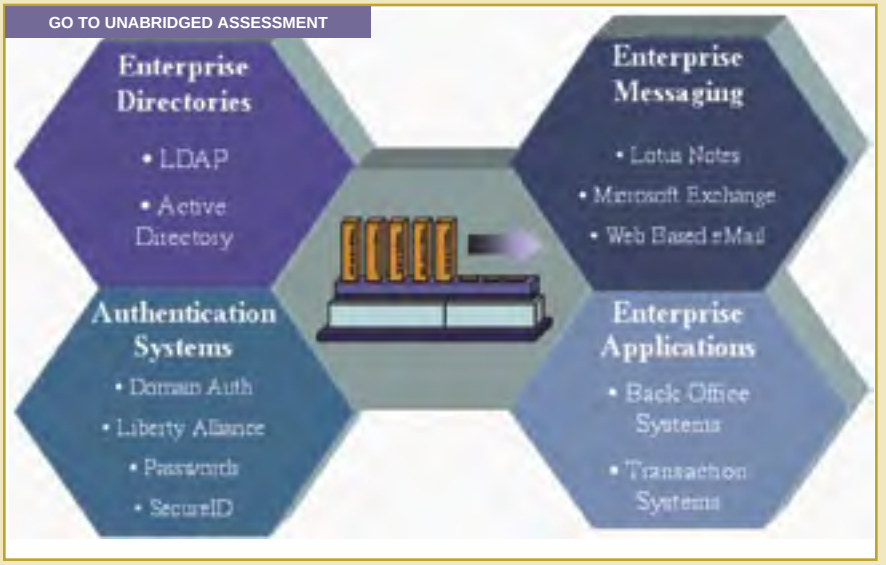
- MDRC2 met stated JWID objectives and provided a graphical user interface to deploy and administer dynamic coalitions while automating the steps necessary to grant a full set of operational privileges based on duty positions.
- While MDRC2 meets functional requirements, it was found to be much more complex than initially anticipated and requires additional development of the graphical user interface.

UST01.09

Voltage Corp. Identity Based Encryption

The VIBE Security Platform provided a means to securing communication without PKI certificate management implementations. VIBE used a public key that did not need to be known or established prior to encrypting a message. This technology stands to significantly reduce requirements for management infrastructure, greatly lowering end user requirements, and allowing the public key to specify policy. Additionally, the platform offered centralized administration and uncomplicated client software setup and utilization plug-ins.

GO TO UNABRIDGED ASSESSMENT



SPONSOR: DARPA, USNORTHCOM
TRIAL LOCATION: USNORTHCOM
TRIAL PARTNERS: UST01.08, UST01.10 UST06.02
OBJECTIVES: Information sharing/multi-level security and ISR dissemination

ASSESSMENT RESULTS: During JWID 2004, VIBE received a warfighter and security assessment and a SEIWG evaluation report.

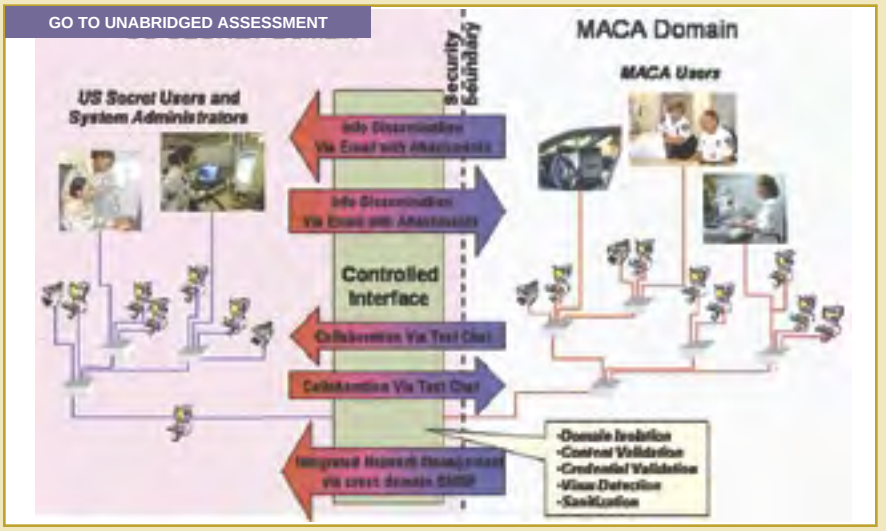
- VIBE successfully demonstrated stated JWID objectives by providing data to users across multiple Internet domains through e-mail encryption using the e-mail address of the recipient as the basis for the encryption key.
- VIBE successfully demonstrated the encrypted transaction of e-mail traffic between Microsoft Outlook and the BlackBerry Exchange Server.
- VIBE is uniquely positioned to support Department of Homeland Security (DHS) organizations requiring data encryption, secure e-mail communications, and external interfaces to BlackBerry or personal digital assistant (PDA) devices.

UST01.10

Multi-Role Boundary Control Information Server Support

MRBC-ISS environment satisfied multiple cross-domain information sharing applications requirements in a single guard solution. The ISSE Guard architecture simultaneously supported a variety of cross domain information exchanges (e-mail, cross domain chat, and network monitoring and management). The ISSE Guard included a cross domain bridge applications suite designed to yield a multi-purpose, high performance, scalable guard architecture capable of simultaneous and secure structured, unstructured and hybrid information transfer.

GO TO UNABRIDGED ASSESSMENT



SPONSOR: DARPA, USNORTHCOM
TRIAL LOCATION: USNORTHCOM
TRIAL PARTNERS: UST01.08, UST01.09 UST06.02
OBJECTIVES: Information sharing/multi-level security

ASSESSMENT RESULTS: During JWID 2004, MRBC-ISS received a warfighter and security assessment and a SEIWG evaluation report.

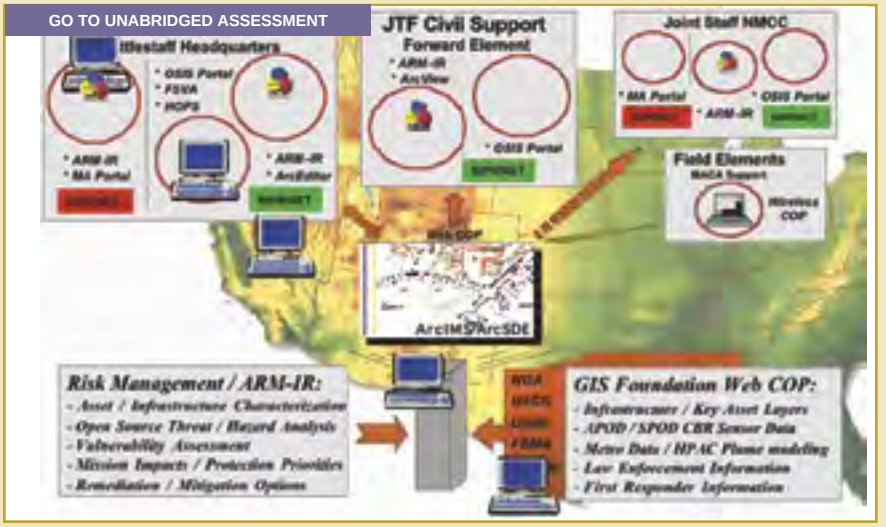
- MRBC-ISS was successful in demonstrating stated JWID objective.
- The MRBC-ISSE Guard provided a suite of cross-domain bridge applications designed to yield a multipurpose, high performance, scalable guard architecture. The system was capable of simultaneous secure transfer of structured information (such as network monitoring information), unstructured information (such as text chat) and hybrid information (such as e-mail with attachments).

UST01.12

Mission Assurance Decision Support Capability Suite

MADS/CS was designed to demonstrate a interoperable decision support capability for homeland defense and civil support missions and enhance operational planning/support for domestic emergencies. It focused on six key elements: risk analysis/management; COP development; infrastructure vulnerability assessment; regionally focused threat/ hazard collection; operational mission planning; and CBR sensor integration. MADS/CS provided "leave behind" elements (CONOPs, TTPs, procedures, and tools) for homeland defense and civil agencies.

GO TO UNABRIDGED ASSESSMENT



SPONSOR: USNORTHCOM
TRIAL LOCATION: USNORTHCOM; DISA Eagle; NSWC Dahlgren; ESC Hanscom
TRIAL PARTNERS: UST01.02, UST02.06, UST02.08, UST02.12
OBJECTIVES: Information sharing/multi-level security, situational awareness, and wireless security

ASSESSMENT RESULTS: During JWID 2004, MADS/CS received a warfighter and interoperability assessment .

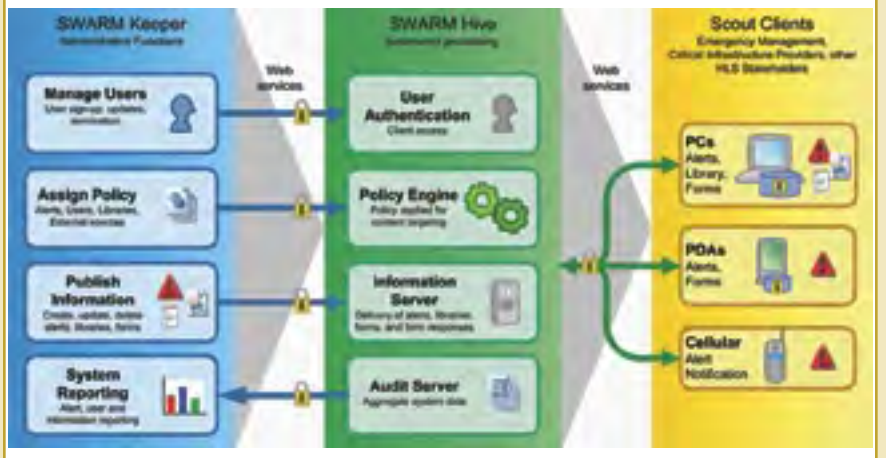
- MADS/CS successfully met stated JWID objectives by demonstrating the ability to collect data from many sources, perform analysis on the data received, and post to a server that was accessible to many users as a Web based COP.
- Demonstrated secure mobile access of MADS/CS WebCOP through a wireless access point which permitted viewing of all data posted to the WebCOP.
- ARM/IR was an outstanding tool for threat and vulnerability analysis and for designing countermeasure packages. This component helped immensely with visualization of threats and solutions.

UST01.13

Secure Wide Area Response Management

SWARM was designed to allow organizations to selectively share and protect sensitive information with HLS stakeholders who provide structured situational awareness forms back to Command and Control for aggregation and fusion as well as securely deliver targeted pre-positioned information and common alerting protocol compliant notification. Shared information included structured data from civilian first responders and local and regional information integration with 9-1-1 centers and state emergency management offices.

GO TO UNABRIDGED ASSESSMENT



SPONSOR: DISA
TRIAL LOCATION: USNORTHCOM; DISA Eagle; NSWC Dahlgren
TRIAL PARTNERS: UST01.02, UST02.09
OBJECTIVES: Information sharing/multi-level security and ISR dissemination

ASSESSMENT RESULTS: During JWID 2004, SWARM received a warfighter, interoperability, and security assessment.

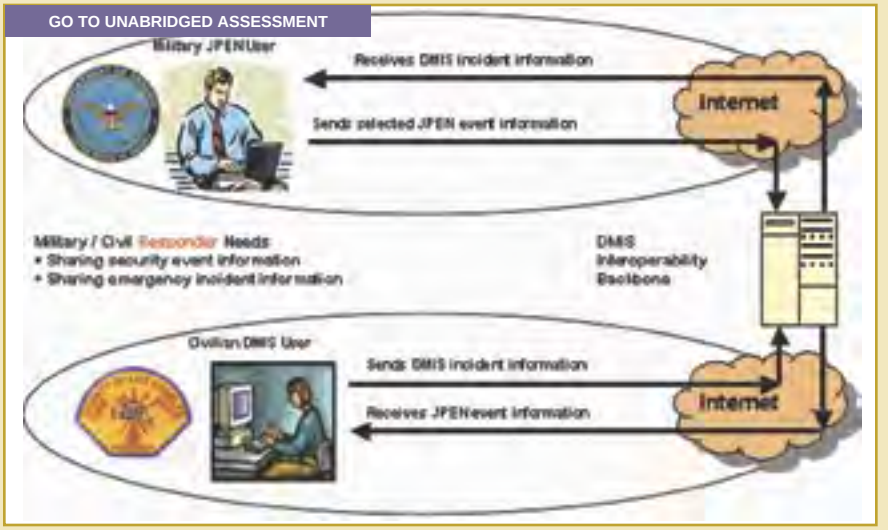
- SWARM successfully demonstrated stated JWID objectives while greatly enhancing the warfighters' ability to achieve their mission providing military assistance to civilian authorities.
- The trial successfully demonstrated that users without proper view permissions were unable to find SWARM data through the encryption layers. Users could not copy/cut or paste from a file provided through SWARM.
- SWARM proved a very useful tool that would benefit the HLS/HLD community.

UST01.14

Disaster Management Interoperability Service

DMIS provided an interoperability infrastructure enabling information sharing among disparate automated systems supporting homeland defense and security. DMIS published interface specifications that enabled external automated systems to "plug in" and share information, provided basic tools to facilitate capture of emergency incident common operating pictures, and enabled shared situation awareness. Working with JPEN (UST02.06) DMIS enabled civilians to receive important security event information from the military.

GO TO UNABRIDGED ASSESSMENT



SPONSOR: USMC
TRIAL LOCATION: USNORTHCOM; DISA Eagle; NSWC Dahlgren
TRIAL PARTNERS: UST02.06
OBJECTIVES: Information sharing/multi-level security

ASSESSMENT RESULTS: During JWID 2004, DMIS received a warfighter and interoperability assessment.

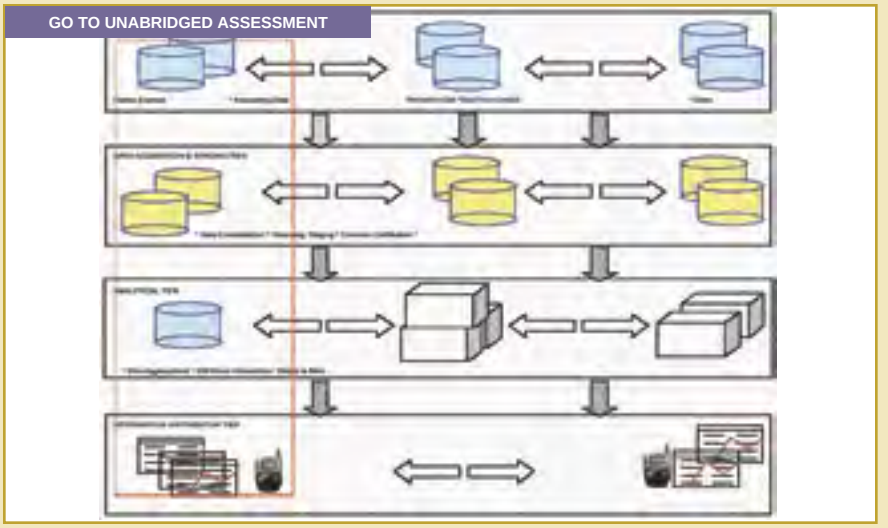
- DMIS successfully demonstrated stated JWID objectives by providing interoperability infrastructure enabling information sharing among disparate automated systems supporting homeland defense and security.
- DMIS Application Tool Suite provided basic responder tools to facilitate capture of the emergency incident common operating picture and enabled shared situational awareness throughout a response force.
- DMIS clearly facilitated a detailed situational awareness/common operational picture (COP) of the National Capital Region (NCR) for USNORTHCOM.

UST01.15

Business Continuity Planning Virtual Command Center

BCP VCC provided users the ability to share information via web and wireless enabled devices to facilitate quick decisions without physical command center presence. BCP VCC capabilities included: Information sharing across multiple information domains; enhanced interoperable situation awareness; solutions to permit enhanced sharing/dissemination of intelligence, surveillance, and reconnaissance products; solutions to address in-transit security of information; solutions to create a fused logistical status; and data collection from various sources and platforms.

GO TO UNABRIDGED ASSESSMENT



SPONSOR: USMC
TRIAL LOCATION: NSWC Dahlgren
TRIAL PARTNERS: UST02.06
OBJECTIVES: Situational awareness

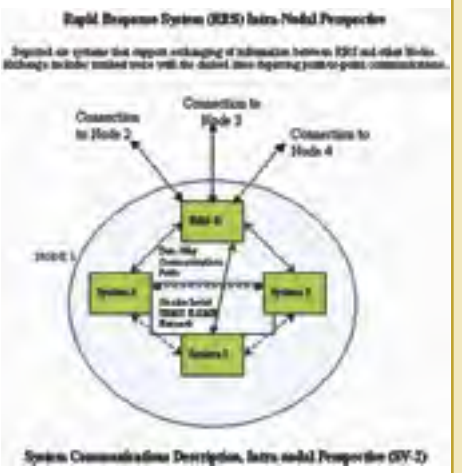
ASSESSMENT RESULTS: During JWID 2004, BCP VCC received a warfighter and interoperability assessment.

- BCP-VCC successfully met stated JWID objectives by allowing users, including operators and first responders, to share information via web enabled and wireless enabled devices without the requirement to be physically present at the command center.
- It provided detailed information sharing on occurring crises, providing the Command Center the ability to rapidly alert large numbers of first responders.
- BCP VCC was portable, but the information shared was limited by the small screen text capability of the wireless phone.

UST02.02
Rapid Response System - Deployable

RRS-D utilized a transportable radio frequency trunking capability to provide on-site voice communications to first responder forces as well as interoperability across all political boundaries. This system was designed to allow "on-site" interoperability and voice communications between USMC emergency services and other federal, state and local agencies involved in public safety. Additionally, RSS-D provided interoperability between other services and agencies.

GO TO UNABRIDGED ASSESSMENT



SPONSOR: USMC
TRIAL LOCATION: NSWC Dahlgren
TRIAL PARTNERS: UST02.15
OBJECTIVES: Situational awareness and ISR dissemination

ASSESSMENT RESULTS: During JWID 2004, RRS-D received a warfighter, interoperability and security assessment.

- RRS-D successfully demonstrated its stated JWID objectives.
- RRS-D successfully provided communication interfaces between state, local and federal communications systems by connecting land mobile radios into a public switch telephone network, connecting dissimilar radio systems to one another, and operating LMRs at different levels of security.
- It increased overall Homeland Security/ Homeland Defense situational awareness levels by providing vertical and horizontal command and control to "on-site" local first responders via a wireless voice network.

UST02.05
Integrated Information Management System

IIMS was designed to help expeditionary and incident response sites (air bases or ports) plan for, protect against, continue operations during, and recover from chemical, biological or conventional attacks. IIMS replaced manual reporting with computer-based data entry and display capabilities, and provided situational awareness with decision tools. The critical enabler was the IIMS Digital Dashboard. Users manually entered data, managed attack and hazard data, reconnaissance reports, and hazard modeling, producing a tailorable common operational picture.

GO TO UNABRIDGED ASSESSMENT

SPONSOR: USAF
TRIAL LOCATION: USNORTHCOM; DISA Eagle; NSWC Dahlgren; SPAWAR; ESC Hanscom
TRIAL PARTNERS: UST01.04, UST02.07
OBJECTIVES: Situational awareness

ASSESSMENT RESULTS: During JWID, IIMS received a warfighter, interoperability and security assessment.

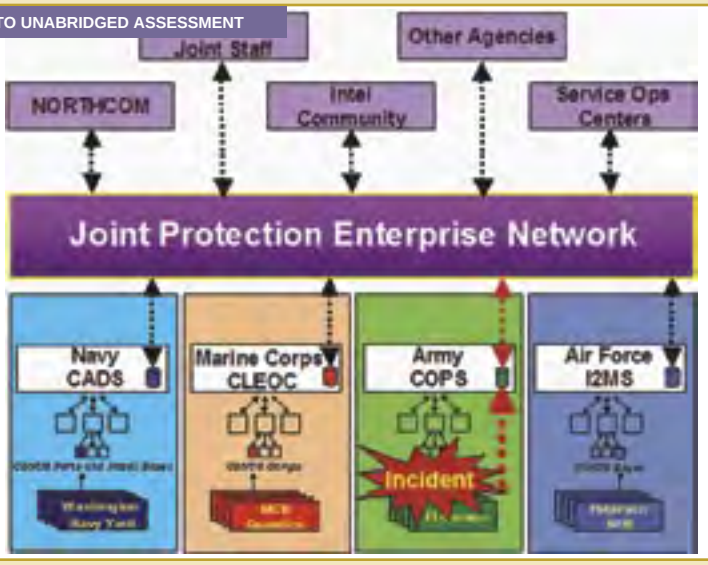
- IIMS partially demonstrated the ability to receive track data for display on IIMS COP. Operators attempted to receive data from Total Domain (UST02.07), but interface problems prevented transfer. IIMS was able to share HPAC Plume and wireless sensor data with all users.
- It includes a useful mapping tool that provided warfighters value-added for plotting incidents and reports, but the capability was not used to full potential.

UST02.06

Joint Protection Enterprise Network

JPEN architecture allowed authorized subscribers to immediately share AT/FP events among DoD installations, operations centers, and intelligence activities, enabling more timely and informed AT/FP posture decisions. JPEN's transformational nature addressed process, people, and technological challenges within DoD and broke down the current Service-centric, hierarchical reporting structure used by installations. JPEN shared information included all types of suspicious activities related to terrorist activities directed against guarded facilities.

GO TO UNABRIDGED ASSESSMENT



SPONSOR: US Joint Staff, USNORTHCOM
TRIAL LOCATION: USNORTHCOM; DISA Eagle; NSWC Dahlgren
TRIAL PARTNERS: UST02.09, UST01.12, UST01.14
OBJECTIVES: Situational awareness and ISR dissemination

ASSESSMENT RESULTS: During JWID 2004, JPEN received a warfighter and interoperability assessment.

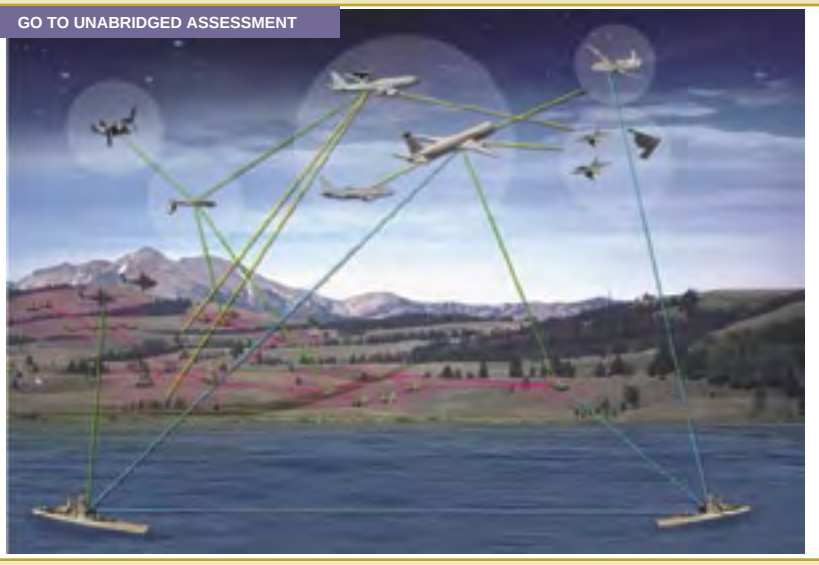
- JPEN successfully demonstrated stated objectives and provided an effective means for alerting and reporting AT/FP events among Service and DoD organizations that does not exist today.
- Increased critical information sharing supporting AT/FP operations to enhance situational awareness.
- The trial queried the network user database looking for patterns of suspicious behavior to provide AT/FP alerts for other participating trials. In that way it enhanced overall ISR.

UST02.07

Total Domain

Total Domain was designed as an Enterprise Application Integration solution, connecting business and mission-critical systems in a scalable, cross-platform messaging infrastructure. Total Domain acted as a data broker, collecting operations data from numerous sources and distributing this data, e-mail and chat functionality, in real time, through multiple organizations and through the use of CIT01.20 on differing security levels. Users could customize core functionality and adapt its operation to specific program requirements while facilitating distributed development and testing.

GO TO UNABRIDGED ASSESSMENT



SPONSOR: USNORTHCOM
TRIAL LOCATION: USNORTHCOM; DISA Eagle; NSWC Dahlgren; ESC Hanscom
TRIAL PARTNERS: CIT01.20
OBJECTIVES: Situational awareness

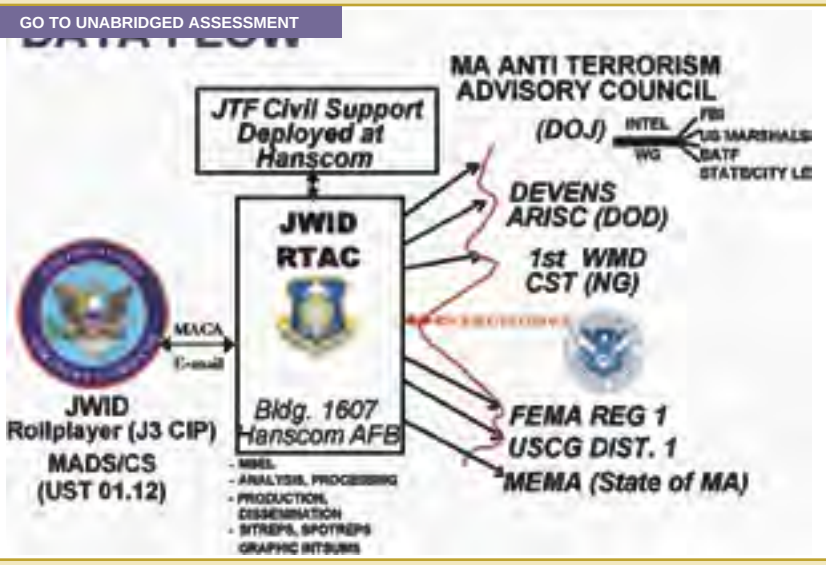
ASSESSMENT RESULTS: During JWID 2004, Total Domain received a warfighter and interoperability assessment.

- Total Domain successfully demonstrated the stated JWID objective, enhancing situational awareness in a Information sharing/multi-level security environment by providing interoperability between local, state, and federal agencies. The one area that Total Domain was not successful in was distributing data beyond their own system. There was an attempt to share the COP data collected by Total Domain with UST02.05 which was unsuccessful due to inability to resolve the data interface.
- The trial provided real-time distribution of multi-formatted data between disparate organizations supporting HLS/HLD.
- It successfully distributed data across security domains based on data filtering and threatcon level policies.

UST02.08
Regional Threat Analysis Cell

RTAC was designed to provide preparation for, prevention of, deterrence of, preemption of, defense against, and response to threats and aggression as well as crisis management, consequence management, and other domestic civil support. The RTAC construct provided a regionally based, CONUS-wide, integrated DoD analytical effort supporting federal/ state/ local civil agencies to develop terrorism situational awareness utilizing existing infrastructure. RTAC supported horizontal and vertical information exchange and common operational view.

GO TO UNABRIDGED ASSESSMENT



SPONSOR: USAF
TRIAL LOCATION: ESC Hanscom
TRIAL PARTNERS: UST01.09
OBJECTIVES: Situational awareness and ISR dissemination

ASSESSMENT RESULTS: During JWID 2004, RTAC received a SEIWG evaluation report.

- RTAC successfully demonstrated stated JWID objectives.

- Enhanced situational awareness by disseminating and receiving regionally relevant Spot Reports (SPOTREP) aligned with the overall scenario and an interactive threat summary matrix to regional participants and to role players at the other JWID sites through encrypted (VIBE UST 01.09) and unencrypted e-mail.

UST02.09
Area Security Operations Command and Control

ASOCC provided real-time, interoperable alerting, collaboration, and visualization capabilities for force protection, homeland defense, and MACA missions at home and abroad. The system was a package of COTS and GOTS software incorporating command and control tools and connectivity to help prevent disasters and facilitate faster emergency response. ASOCC supports operations of: U.S. Combatant Commanders; U.S. federal partners; host nation security forces overseas; and military Services and federal, state, and local partners in the U.S.

GO TO UNABRIDGED ASSESSMENT

SPONSOR: USNORTHCOM
TRIAL LOCATION: USNORTHCOM; DISA Eagle; NSWC Dahlgren
TRIAL PARTNERS: UST01.02, UST01.13, UST02.06, UST02.16
OBJECTIVES: Information sharing/multi-level security, situational awareness and ISR dissemination

ASSESSMENT RESULTS: JWID 2004, ASOCC received a warfighter and interoperability assessment.

- ASOCC successfully provided enhanced Homeland Security and Homeland Defense situational awareness through effective status/event reporting, visual imagery/data displays, map plotting, and chat functions.

- The trial provided real-time alerting and event visualization capabilities in support of DoD's homeland defense and civil support missions. It presented track/location visual display using XIS as an alternate to the GCCS COP.

UST02.11

Weapons of Mass Destruction Common Operational Picture Support

WMD Common Operational Picture Support provided a decision tool for Consequence Management and WMD planning/crisis management accessible from within a common operational viewer. Using the Defense Threat Reduction Agency's dispersion models, analysts had the ability to present WMD-related planning information directly to, and embedded within, a common operational picture platform. Through embedded COP products, the decision maker could see the problem as it related to the mission, thereby enhancing response and mitigating effects.

GO TO UNABRIDGED ASSESSMENT

SPONSOR: USNORTHCOM
TRIAL LOCATION: USNORTHCOM
TRIAL PARTNERS: UST02.16
OBJECTIVES: Situational awareness

ASSESSMENT RESULTS: During JWID 2004, WMD COP was scheduled to receive a warfighter and interoperability assessment.

- An interoperability assessment was performed on this trial although system-to-system data exchange was not performed since the data format of the receiving system was not acceptable. Due to this the utility of data was assessed but not exchange of data.
- While the WMD COP provided data to HLD COP during JWID execution the systems were not connected and therefore WMD did not demonstrate any interoperability that could be assessed.
- It was determined at JWID execution that the trial did not warrant a warfighter assessment based on the lack of warfighter interaction that was not previously disclosed to the assessment team.
- The trial proved to be a concept development platform.

UST02.12

Regional Information Joint Awareness Network

RIJAN was designed to facilitate information exchange between command nodes throughout the life cycle of a crisis, from initial threat indication through disaster response and recovery while providing consequence management, planning, training, response management and common situational awareness across the region. Sharing sensor data feeds across organizational domains to support an RCOP, RIJAN identified best of breed/common/interoperable collaboration tool capabilities, provided incident management tools, and mapping tools.

GO TO UNABRIDGED ASSESSMENT

SPONSOR: US Army
TRIAL LOCATION: USNORTHCOM; DISA Eagle; NSWC Dahlgren
TRIAL PARTNERS: UST01.13, UST02.08, UST02.09, UST04.01, UST04.03
OBJECTIVES: Situational awareness and ISR dissemination

ASSESSMENT RESULTS: During JWID 2004, RIJAN received a warfighter and interoperability assessment.

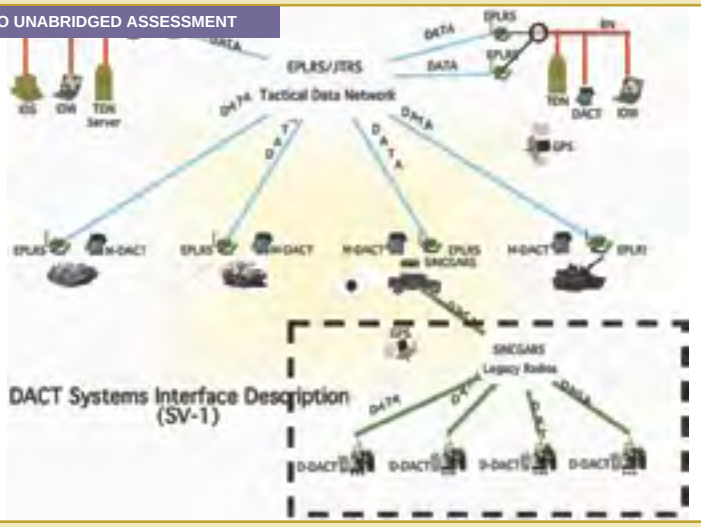
- RIJAN successfully demonstrated stated JWID objectives by providing an actual situational awareness picture of the New York/New Jersey metropolitan area to USNORTHCOM through the Network Centric Enterprise capabilities.
- RIJAN exceeded the expectations of warfighters by demonstrating the ability of Federal, State and local agencies leveraging existing resources to achieve a common goal.

UST02.15

Dismounted Data Automated Communications Terminal

The D-DACT was designed as a small, handheld, Ruggedized Personal Digital Assistant device with enhanced battery life, carried by individual Marines. Utilizing Windows Command and Control Compact Edition (C2CE), the application adapts key components of the C2PC application and provides automated communications support for commanders in tactical operations. Using GPS data, D-DACT displayed its own location on the C2 network and provided VMF message, route and overlay, and friendly and enemy position information enhancing situational awareness.

GO TO UNABRIDGED ASSESSMENT



SPONSOR: USMC
TRIAL LOCATION: NSWC Dahlgren
TRIAL PARTNERS: N/A
OBJECTIVES: Information sharing/multi-level security, situational awareness and ISR dissemination

ASSESSMENT RESULTS: During JWID 2004, D-DACT received a warfighter and interoperability assessment.

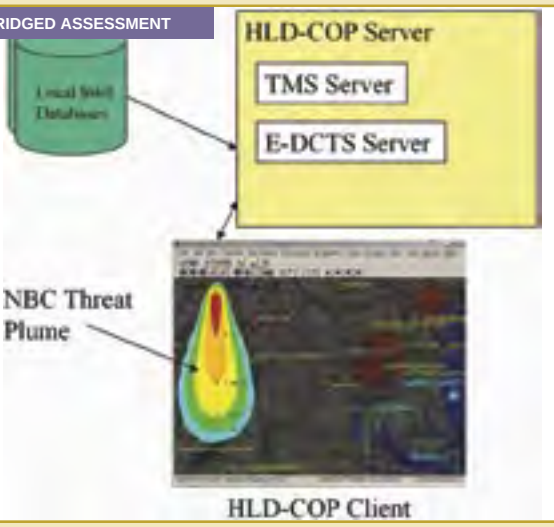
- D-DACT successfully demonstrated stated JWID objectives by providing a wireless messaging capability, real-time locations of first response personnel on a hand-held PDA COP with a simple interface for transmitting reports.
- Utilizing PDAs functioning as GPS units, all first responder's positional data was displayed on a COP within their own PDA. The information was also transmitted and shared through a wireless access point inside the Dahlgren JWID facility for format conversion compatible with the TOPCOP.

UST02.16

Homeland Defense Common Operational Picture Workstation

HLD Common Operational Picture (HLD COP) Workstation provided enhancements to the current GCCS system used to display military unit positions with extra information sources and features for use in Homeland Defense. Its ability to view Nuclear, Biological, and Chemical threat plumes as well as enhancements allowing greater access to local intelligence databases greatly increased the users situational awareness. HLD COP also supported collaboration with other operators through an enhanced on-line defense collaboration system.

GO TO UNABRIDGED ASSESSMENT



SPONSOR: USNORTHCOM
TRIAL LOCATION: USNORTHCOM; DISA Eagle; NSWC Dahlgren
TRIAL PARTNERS: UST01.02, UST01.13, UST02.09
OBJECTIVES: Situational awareness and ISR dissemination

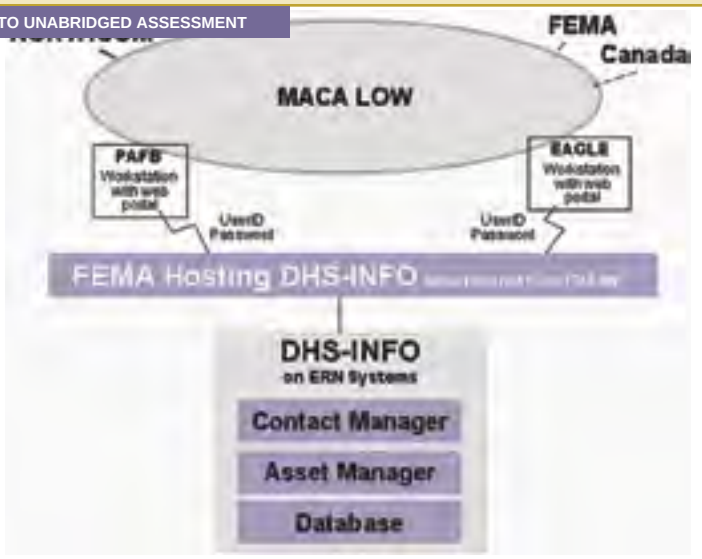
ASSESSMENT RESULTS: During JWID 2004, HLD COP received a warfighter and interoperability assessment.

- HLD COP successfully demonstrated stated JWID objectives by providing enhancements to GCCS for a more flexible tailoring of the track displays than is currently available with GCCS 3.6.
- The trial provided an Enhanced Integrated Intelligence and Imagery (I3) functionality allowing Intel records and Imagery to be associated with tracks.
- HLD COP systems included the ASOCC eXPanel system for event management and alerting, and allowed users to create queries of local databases.

UST02.18
Emergency Response Network Systems

ERN Systems™ provided a secure, unclassified Alert and Notification/ Information Sharing technology delivering regional and national one-stop access via existing, readily available technology. ERN Systems™ goal was to demonstrate bi-directional information/intelligence collection and dissemination to include Homeland Security/Homeland Defense partners from the private sector as well as in agencies and critical infrastructures. ERN Systems™ was also customizable for unique or multilevel commands.

GO TO UNABRIDGED ASSESSMENT



SPONSOR: FBI, FEMA
TRIAL LOCATION: USNORTHCOM; DISA Eagle
TRIAL PARTNERS: N/A
OBJECTIVES: Information sharing/multi-level security and situational awareness

ASSESSMENT RESULTS: During JWID 2004, ERN Systems received a warfighter assessment and SEIWG evaluation report.

- ERN successfully met stated JWID objectives by demonstrating a simple, rapid and efficient way for the warfighter to communicate with the various HLS/HLD agencies.
- ERN provided improved communications with DHS and state emergency centers and demonstrated data sharing through a single virtual database of contacts and assets by way of the “National Interoperability Portal.”
- ERN Systems located at the FEMA regional offices were linked to facilitate a wider search for contacts and assets, simulating what would be required for an actual emergency.

UST04.01
Roaming Emergency Communications Network

RECON provided solutions to permit enhanced sharing/dissemination of intelligence, surveillance, and reconnaissance products within and across coalition and inter-agency information domains. Providing portable broadband wireless communication, RECON enhanced interoperable situational awareness and was scalable in both time and scope, within and between information domains. RECON also allowed real-time data and intelligence information sharing between remotely separated forces and addressed in-transit security between fixed and mobile users.

GO TO UNABRIDGED ASSESSMENT

SPONSOR: US Army
TRIAL LOCATION: DISA Eagle; NSWC Dahlgren
TRIAL PARTNERS: UST02.12
OBJECTIVES: Situational awareness and ISR dissemination

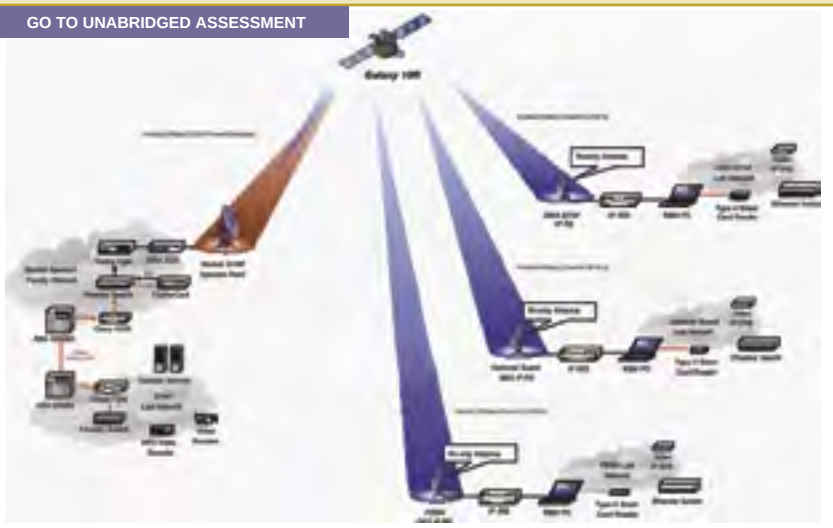
ASSESSMENT RESULTS: During JWID 2004, RECON received a warfighter and interoperability assessment.

- RECON successfully demonstrated stated JWID objectives by providing interoperable communications for non-line-of-sight users through creation of a bridge between the wired networks and the wireless field users.
- RECON successfully provided real-time sharing of data and intelligence information through their Bread crumb technology. This technology utilized cameras which provided real-time situational awareness information on identified events.

UST04.03
GBS Homeland Defense Architecture

Global Broadcast System (GBS) HLD Architecture demonstrated the GBS satellite system broadband delivery capabilities in support of homeland security and U.S. domestic interagency information sharing. The architecture applies technical lessons learned to demonstrate real-time broadcast of broadband Internet Protocol (IP) based content to select domestic response agencies. Using GBS-leased commercial satellite communication resources and COTS Type-II encryption technology, the system broadcasted streaming video, high resolution imagery, and data.

GO TO UNABRIDGED ASSESSMENT



SPONSOR: USAF
TRIAL LOCATION: USNORTHCOM; DISA Eagle; NSWC Dahlgren; ESC Hanscom
TRIAL PARTNERS: UST02.12, CIT04.02
OBJECTIVES: Situational awareness and ISR dissemination

ASSESSMENT RESULTS: During JWID 2004, received a warfighter and interoperability assessment.

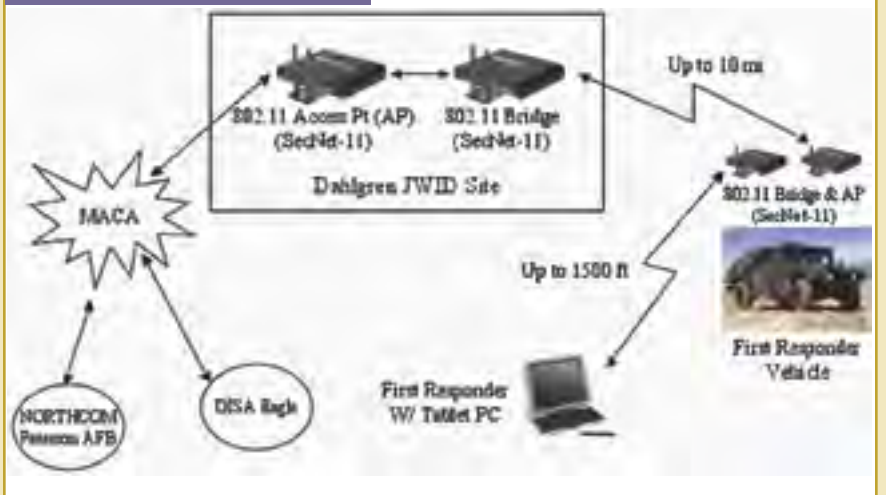
- GBS successfully demonstrated stated JWID objectives while sending videos, imagery and plume data to multiple JWID trials using one-way satellite transmissions as an alternate method of data dissemination.

- GBSs real time video stream feeds proved to be an effective and reliable means of disseminating information to the various HLS agencies.

UST05.02
Geospatial Intelligence Wireless Advanced Imagery Dissemination

GI Secure Wireless Advance Imagery Disseminations goals were to demonstrate the utility of direct data access at classified level “in the field/on the scene,” pull/utilize NGA geospatial intelligence products, interact with personnel and command elements in rear area via real-time VTC; relay that data back to command post; and disseminate imagery via Kodak AGILE JPEG 2000 Compression Application.

GO TO UNABRIDGED ASSESSMENT



SPONSOR: NGA
TRIAL LOCATION: NSWC Dahlgren; NGA
TRIAL PARTNERS: N/A
OBJECTIVES: Wireless security

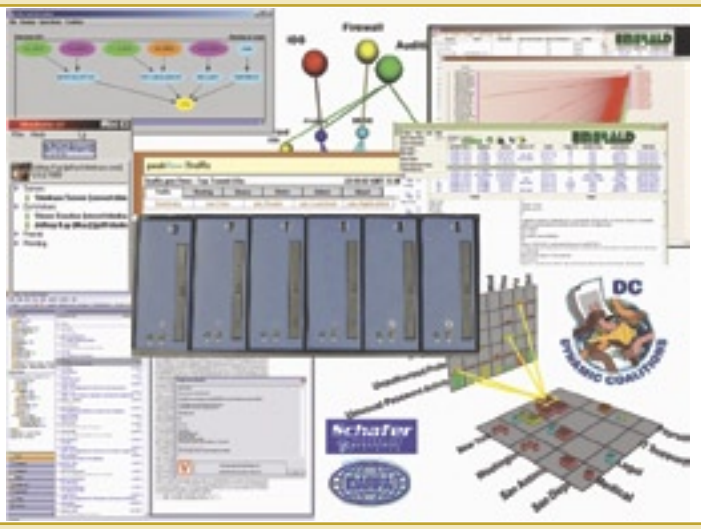
ASSESSMENT RESULTS: During JWID 2004, GI received a warfighter and interoperability assessment.

- GI Secure Wireless successfully demonstrated the stated JWID objective by providing a secure wireless link (MACA network extension) between forward first responders and the Incident Command Post. That link demonstrating direct data access at the “classified level” in the field.

UST06.02

Suite of Operationally Inexpensive Security Hosts

SOISH was designed as an adaptable application platform that can be tailored to provide comprehensive computer network defense capabilities. The SOISH concept promoted highly modular, adaptable computing to support network-centric warfare, while providing great application support flexibility. SOISH also utilized controlled information sharing facilities, network traffic analysis capability, data visualization for graphical correlation of attack data, and intrusion prevention services provided by host-based hardware firewalls.



SPONSOR: DARPA
TRIAL LOCATION: USNORTHCOM; DISA Eagle; SPAWAR
TRIAL PARTNERS: UST01.08, UST01.09, UST01.10
OBJECTIVES: Coalition network defense

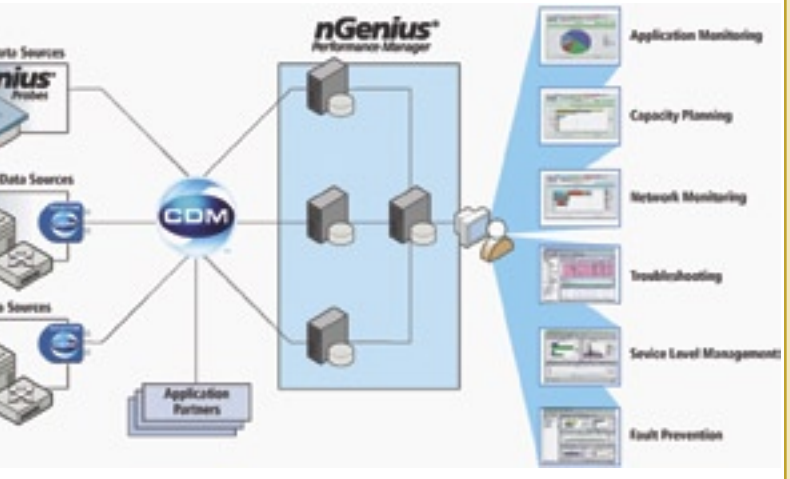
ASSESSMENT RESULTS: During JWID 2004, SOISH received a warfighter assessment and SEIWG evaluation report.

- SOISH successfully demonstrated its stated JWID objective while providing a suite of computer network defense tools which the warfighters viewed as viable solutions for monitoring and defending against multiple threats.
- Secure Spread, another feature of SOISH, performed successfully, presenting the visual network connectivity status for the MACA network.

UST06.03

NetScout Performance Manager 2.01

NetScout provided a comprehensive hardware and software solution to simplify complex enterprise networks management and provide visibility into the entire network. The software component, nGenius Performance Manager combined real-time and historical information on a single platform for network and application monitoring, troubleshooting, capacity planning, fault prevention, and service level management. The hardware component, nGenius Probes, non-intrusively monitored traffic flows throughout the network core, distribution, access and storage areas.



SPONSOR: DISA
TRIAL LOCATION: DISA Eagle; NSWC Dahlgren; SPAWAR
TRIAL PARTNERS: N/A
OBJECTIVES: Coalition network defense

ASSESSMENT RESULTS: During JWID 2004, NetScout received a warfighter assessment and SEIWG evaluation report.

- NetScout successfully met their stated JWID objective by providing a powerful and easy to use tool for network analysis. It provided a system to monitor network applications and bandwidth usage that could be used as a core network solution for implementation on operational networks.
- nGenius Performance Manager monitored network activity and identified application degradations to pinpoint anomalies before user productivity was impacted.

CIT CONTENTS

Coalition Assessment Briefs

COALITION INTEROPERABILITY TRIALS

Hanscom AFB, Mass.
SPAWAR, Calif.
Dahlgren, Va.
DISA Eagle, Va.
Peterson AFB, Colo.

Australia
Canada
New Zealand
United Kingdom
NATO

ACRONYMS AND ABBREVIATIONS

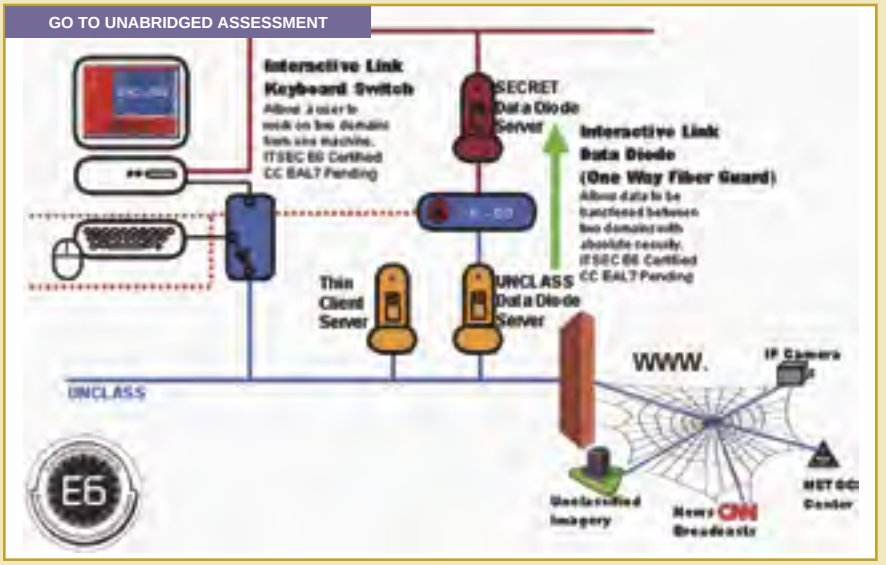
The reference list for the entire report is on the inside back cover of this booklet.

CIT01.01

Interactive Link

The Interactive Link Data Diode provided a one way data connection between two information domains and ensured that high level data did not flow back to the low level domain. A Keyboard Switch component allowed warfighters to work on two information domains from one machine and enabled information to be copied from low-level to high-level using the Windows or Unix clipboard. Utilizing thin client technology, warfighters displayed a low-level window on their high-side workstation and performed web browsing, text chat and e-mail tasks.

GO TO UNABRIDGED ASSESSMENT



SPONSOR: DISA
TRIAL LOCATION: DISA ATIS-JPO; SPAWAR; MNTG SPAWAR; Canada; New Zealand
TRIAL PARTNERS: CIT01.05, CIT01.08, CIT03.04
OBJECTIVES: Information sharing/multi-level security and coalition network defense

ASSESSMENT RESULTS: During JWID 2004, Interactive Link received a warfighter assessment and SEIWG evaluation report.

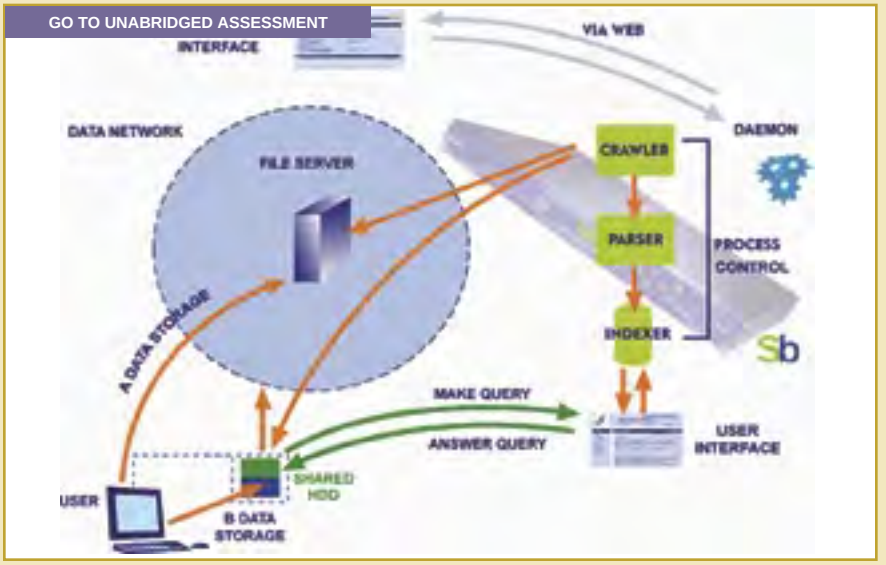
- Interactive Link performed as intended for JWID execution and successfully demonstrated all of its stated objectives.
- Warfighters uniformly agreed that it is a welcome technology and should be implemented now.
- The trial drew interest from the U.S. Navy for ability to securely pass data unidirectionally across domains and ability to access two networks from a single workstation.

CIT01.03

Search Box

Search Box was designed to allow warfighters to retrieve information from the JWID data network by accessing unstructured files in different formats (html, MSOffice, txt, pdf, rtf and ps). Using different interfaces (Web, WAP, PDA), warfighters could find and retrieve files according to parameters, such as content, structure, source, etc. The goals were to demonstrate the tool's efficient resource usage and analysis capability as well as demonstrate the search engines power, format filtering versatility, customization capability, security controls and scalability.

GO TO UNABRIDGED ASSESSMENT



SPONSOR: Spain
TRIAL LOCATION: NSWC Dahlgren; SPAWAR; Canada; Spain; NATO
TRIAL PARTNERS: CIT01.08
OBJECTIVES: Information sharing/multi-level security

ASSESSMENT RESULTS: During JWID 2004, Search Box received a warfighter assessment and SEIWG evaluation report.

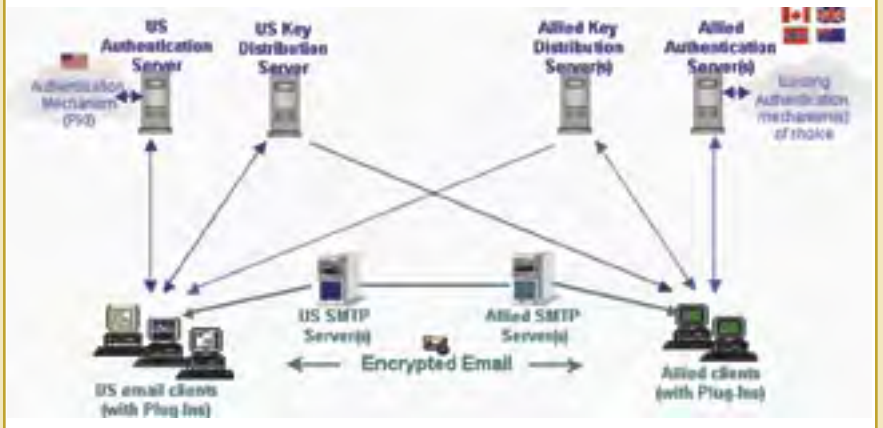
- Search Box successfully demonstrated information sharing across multiple domains by indexing documents and e-mails and providing a search engine to find information through keywords.
- The trial encountered several technical and set up issues throughout JWID execution and lacked vendor support to correct the problems.
- Warfighter questionnaire responses were primarily unfavorable because exposure to the system was limited due to operational problems.

CIT01.05

PKI Express and Interop Express

The PKI trial was designed to facilitate secure message exchange across domains between coalition nations without exposing internal authentication information. Utilizing federated authentication, each ally maintained complete control over its own environment while achieving secure interoperability with other coalition members. Allies accomplished user authentication via their own authentication server, interfacing with their authentication mechanisms. The PKI solution consisted of Sigaba components that could be deployed in different design configurations.

GO TO UNABRIDGED ASSESSMENT



SPONSOR: DISA
TRIAL LOCATION: DISA Eagle; NSWC Dahlgren; SPAWAR; Australia; Canada; New Zealand; United Kingdom; NATO
TRIAL PARTNERS: CIT01.01, CIT01.08, CIT03.03
OBJECTIVES: Information sharing/multi-level security

ASSESSMENT RESULTS: During JWID 2004, The PKI trial received a warfighter and interoperability assessment.

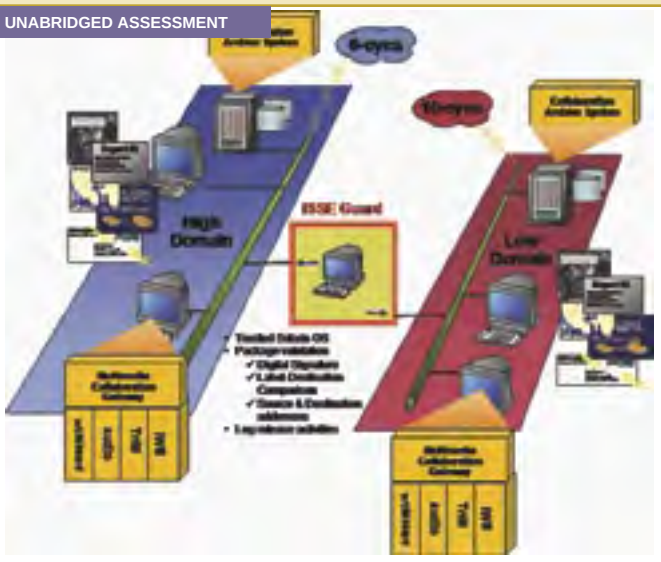
- The PKI trial successfully provided solutions to facilitate information sharing across multiple information domains including defense and other government agencies.
- Provided cross-domain secure SMTP messaging capability without having to rely on a common authentication or PKI infrastructure.
- Warfighters viewed it as a good tool to digitally certify secure information across domains with coalition partners without employing additional hardware or utilizing PKI cards with digital certificates.

CIT01.06

Multimedia Collaborative Gateway

MCG was designed to provide synchronous collaboration across multiple security levels and specifically, enable users on separately classified networks to communicate using text chat/instant messaging and shared whiteboard. During JWID 2004, role players used MCG collaboration tools, to securely share situational awareness and intelligence, surveillance and reconnaissance information. MCG also incorporated the Collaboration Archive System to provide information discovery through a novel, context-sensitive search engine.

GO TO UNABRIDGED ASSESSMENT



SPONSOR: USAF
TRIAL LOCATION: DISA Eagle; Canada
TRIAL PARTNERS: N/A
OBJECTIVES: Information sharing/multi-level security, situational awareness and ISR dissemination

ASSESSMENT RESULTS: During JWID 2004, MCG received a interoperability assessment.

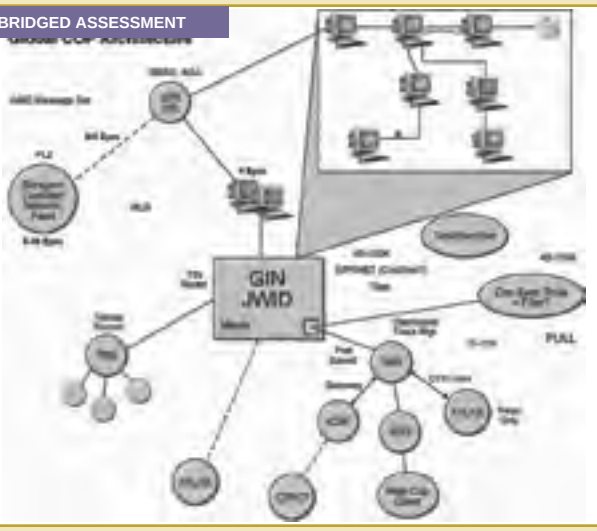
- The MCG trial was partially successful meeting stated JWID objectives.
- MCG used a dummy domain riding on the CFBLnet and the ISSE Guard to successfully demonstrate cross-domain information sharing capability. Although originally intending to demonstrate both text chat and shared whiteboard, MCG only demonstrated text chat using Information Work Space (IWS).
- While originally intending to share/disseminate ISR products, the demonstration was again limited to the XMPP protocol transfer of text chat messages using IWS. The objective was not fully met.

CIT01.07

Joint Deployable Intelligence Support System

JDISS Global COP was billed as the beginning of a solution to take SCI source data and share it at the GENSER, SCI, and releasable levels in a Information sharing/multi-level security environment. JDISS was intended to build the interface between IBS and the GCCS-I3 Middle Tier Services to include WEB COP clients. Inclusive in the Global COP provided server (Cross Domain Server-CDS) was the COP, GMI and Imagery. This capability was intended to facilitate intelligence and information sharing across many domains and security levels.

GO TO UNABRIDGED ASSESSMENT



SPONSOR: US Navy
TRIAL LOCATION: NSWC Dahlgren
TRIAL PARTNERS: N/A
OBJECTIVES: Information sharing/multi-level security and situational awareness

ASSESSMENT RESULTS: During JWID 2004, JDISS Global COP received a SEIWG evaluation report.

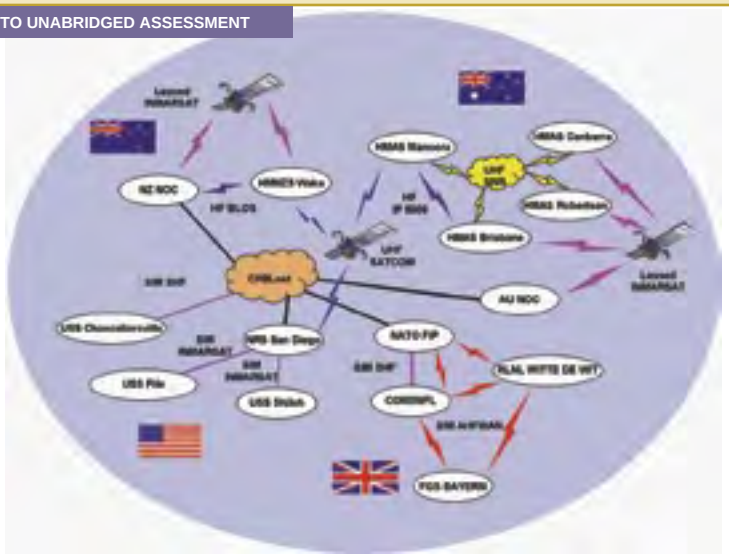
- JDISS did not meet stated JWID objectives.
- Although originally intended to define data and declutter the operational picture on one machine with feeds coming from three different classified domains, JDISS was unable to demonstrate this feature.
- While JDISS personnel stated that JDISS could filter on Target Type, Track ID, GEO Loc and Time/Date, only Target Type could be filtered. Neither the warfighter nor technical representative could filter on Date/Time.

CIT01.08

Multinational Naval Task Group

MNTG and NATO NC3A Allied HF WAN demonstration was an amalgam of C4I capabilities that operated in the low-bandwidth, high latency maritime communications environment. Capabilities included the establishment and operation of a tactical IP network and provision of the applications which supported warfighters with knowledge sharing and situational awareness in an Allied/Coalition environment. MNTG provided an infrastructure to share information in a timely manner, collaborate in real-time, and distribute the COP within a secure tactical IP network.

GO TO UNABRIDGED ASSESSMENT



SPONSOR: MNTG, NATO
TRIAL LOCATION: MNTG SPAWAR; MNTG Australia; MNTG New Zealand; MNTG NATO
TRIAL PARTNERS: CIT01.01, CIT01.03, CIT01.05, CIT02.01, CIT02.10, CIT02.18, CIT03.03, CIT03.04
OBJECTIVES: Information sharing/multi-level security, situational awareness, wireless security and coalition network defense.

ASSESSMENT RESULTS: During JWID 2004, MNTG received a SEIWG evaluation report.

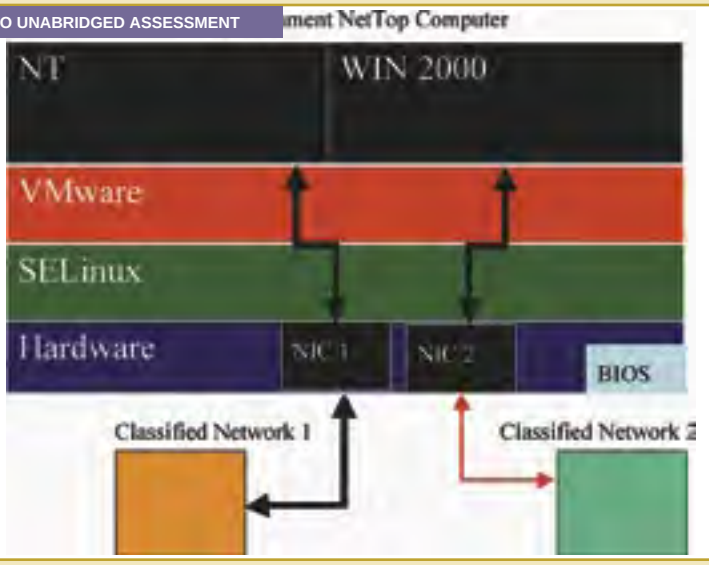
- MNTG successfully demonstrated all stated JWID objectives and successfully validated the routing architecture and multicast support.
- Subnet Relay - In Australia, SNR was successfully used to provide a simulated ship with connectivity to the MNTG network via a gateway ship to support e-mail, multicast chat (Mchat) and Sametime Text Chat.
- MNTG incorporated several CITs that allowed them to demonstrate interoperability and value to the warfighter.

CIT01.10

NetTop

Designed as a multiple domain access workstation, NetTop provided JWID warfighters the ability to simultaneously access to multiple networks while operating from a single workstation. Comprised of commercial-off-the-shelf (COTS) intelligence hardware, SELinux, and VMware Workstation, it provided desktop reduction through the use of virtual separation.

GO TO UNABRIDGED ASSESSMENT



SPONSOR: NSA
TRIAL LOCATION: USNORTHCOM; DISA Eagle; NSWC Dahlgren; SPAWAR; Canada
TRIAL PARTNERS: UST02.09, CIT04.03
OBJECTIVES: Information sharing/multi-level security

ASSESSMENT RESULTS: During JWID 2004, NetTop received a warfighter assessment and SEIWG evaluation report.

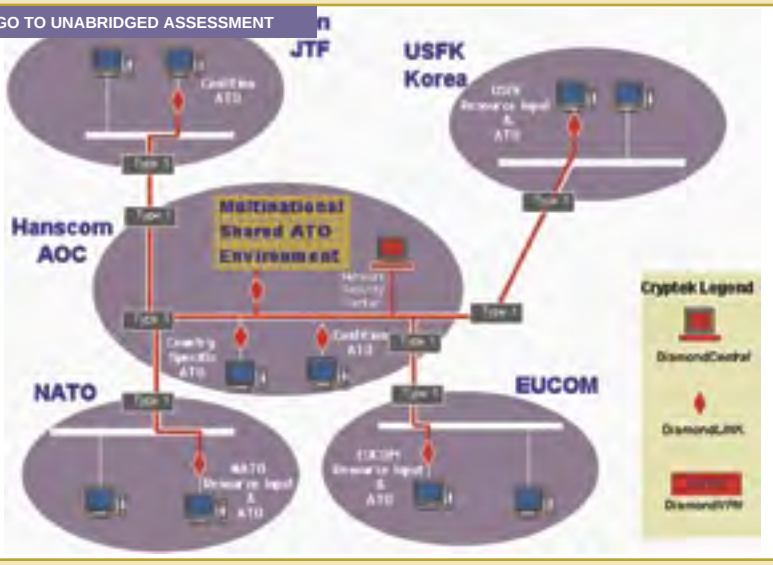
- NetTop successfully met the stated JWID objective by demonstrating dual domain information sharing with two of the three JWID domains through the use of VMware and SELinux software.
- The trial successfully provided ability to view multiple domains from a single workstation.
- NetTop proved to be easily deployable as it can be installed on existing hardware platforms without additional hardware requirements.

CIT01.19

Coalition Secure Interoperability

CSI demonstrated the ability to eliminate multiple data bases by allowing storage of data with different security level labels in one common data base. Utilizing Oracle's new "9i" database CSI placed labeled data in a shared disk array, which appeared as one virtual database and provided the capability to protect data at different security levels. This technology permitted a person with any security level on the network to see only the data that was releasable to that security level.

GO TO UNABRIDGED ASSESSMENT



SPONSOR: USAF
TRIAL LOCATION: NSWC Dahlgren; ESC Hanscom; USFK; Canada; NATO
TRIAL PARTNERS: N/A
OBJECTIVES: Information sharing/multi-level security, database fusion and ISR dissemination

ASSESSMENT RESULTS: During JWID 2004, CSI received a warfighter assessment and SEIWG evaluation report.

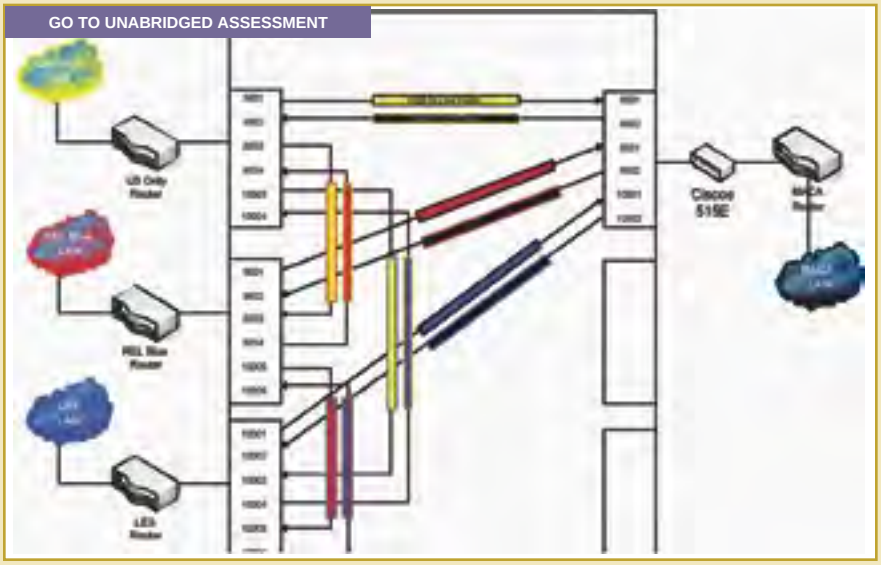
- CSI successfully met stated JWID objectives by facilitating ISR dissemination in a Information sharing/multi-level security environment by data labeling information in a common database and using pre-defined security access level common access cards (CAC).
- Warfighters were impressed with its ability to limit access to information on a need to know basis, quickly search a common database for pertinent ATO information and view supporting data, (i.e. unit location, unit number of aircraft assigned, etc).

CIT01.20

Secure Network Server

SNS was designed to facilitate automated information sharing among networks operating at multiple information security levels by enforcing independent security policies between each information security level. To accomplish this, security administrators for each network and Designated Approving Authority representatives agreed on their respective security policies for sharing information and SNS was configured to enforce these policies. This allowed information to flow across multiple domains at available network bandwidth speeds with minimal security risks.

GO TO UNABRIDGED ASSESSMENT



SPONSOR: USNORTHCOM
TRIAL LOCATION: USNORTHCOM; DISA Eagle; NSWC Dahlgren; SPAWAR; ESC Hanscom
TRIAL PARTNERS: UST02.07
OBJECTIVES: Information sharing/multi-level security

ASSESSMENT RESULTS: During JWID 2004, SNS received an interoperability and security assessment.

- SNS successfully met the stated JWID objective by establishing three dummy domains within the JWID MACA domain and allowing for passage of text chat messages, e-mail and track data to the Boeing VCN COP display based on the differing classifications of each dummy domain.

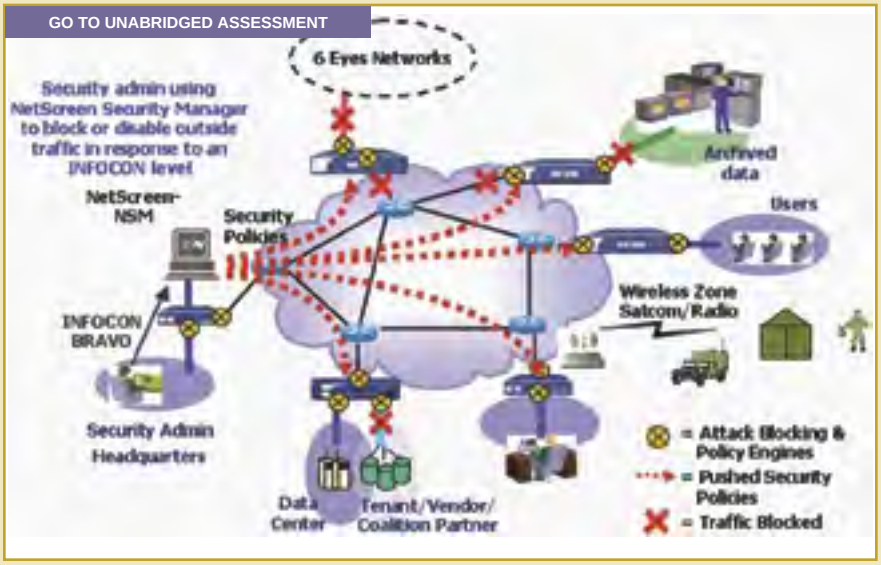
- Information generated at lower levels of security were seamlessly transmitted to higher levels while information generated at higher levels of security was sanitized and transmitted appropriately to the lower security levels.

CIT01.22

Netscreen Technologies

Netscreen was designed to provide a purpose-built security system, integrating a stateful inspection firewall, Virtual Private Network (VPN), denial of service protection, deep packet inspection and traffic management. The trial demonstrated the ability to create a community of interest through the use of VPNs, the ability to add and remove users within a VPN and the ability to permit entire enclaves or individual access. Netscreen also addressed network security through a firewall to prevent unauthorized access, while monitoring for known attack signatures.

GO TO UNABRIDGED ASSESSMENT



SPONSOR: USNavy, UK
TRIAL LOCATION: SPAWAR; Canada; New Zealand; United Kingdom
TRIAL PARTNERS: N/A
OBJECTIVES: Information sharing/multi-level security and wireless security

ASSESSMENT RESULTS: During JWID 2004, Netscreen Technologies received a SEIWG evaluation report.

- Netscreen Technologies successfully demonstrated all stated objectives through creation and management of VPNs in both conventional and wireless environments.

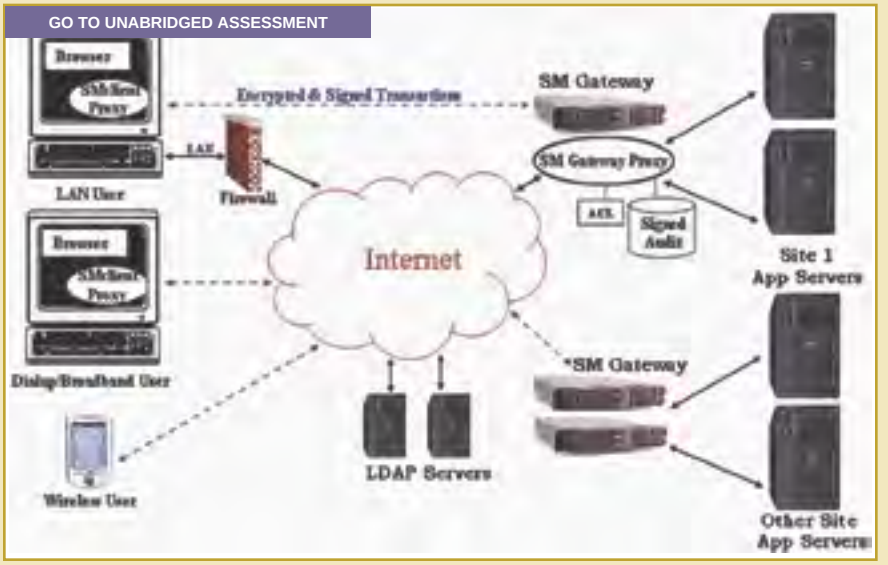
- Netscreen's firewall product and the accompanying management suite provided warfighters an easy means of operating and administering functions over existing firewall products.

CIT01.25

Secure Methods SM 1000 Gateway

Secure Methods provided strong security without requiring any action or intervention on the part of users or system administrators. The two main components were a gateway appliance component and a client component. The SM Gateway enabled users to authenticate, authorize, audit, digitally sign, and encrypt transaction data in a legally enforceable manner. Utilizing no-cost client software, users transparently added digital signatures and strong encryption, authentication, authorization and audit services to fully secure all e-business applications.

GO TO UNABRIDGED ASSESSMENT



SPONSOR: JITC
TRIAL LOCATION: NSWC Dahlgren; SPAWAR; Australia; NATO
TRIAL PARTNERS: N/A
OBJECTIVES: Information sharing/multi-level security

ASSESSMENT RESULTS: During JWID 2004, SM Gateway received a security assessment and SEIWG evaluation report.

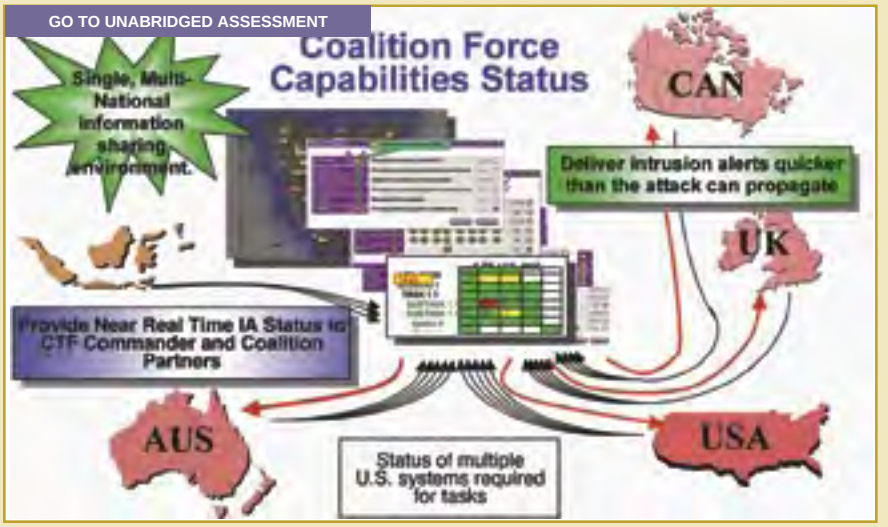
- Secure Methods successfully demonstrated the stated JWID objective by creating a security infrastructure including embedded PKI and digitally signed audit trails.
- Warfighters were able to access secure information stores where they were given access or were denied access based on their credentials.
- The SM1000 Gateway provided an easy-to-deploy, easy-to-install, cost effective solution for providing secure, audited transactions.

CIT02.01

Coalition-Information Assurance Common Operational Picture

C-IA COP facilitated technology information multilateral sharing while protecting national sovereignty, analyzing critical technical infrastructures supporting the CTF commander's mission and providing early warning of potential attacks on the coalition forces' technical infrastructure. C-IA COP interfaced with coalition systems for status and networks reporting and correlated to current mission-critical tasks. C-IA COP also provided tools to enforce data-sharing agreements and policy to share sanitized IA situational awareness information.

GO TO UNABRIDGED ASSESSMENT



SPONSOR: DISA
TRIAL LOCATION: NSWC Dahlgren; SPAWAR; MNTG SPAWAR; ESC Hanscom; MNTG Australia; New Zealand; MNTG New Zealand; United Kingdom: NATO; MNTG NATO
TRIAL PARTNERS: N/A
OBJECTIVES: Information sharing/multi-level security, situational awareness and coalition network defense

ASSESSMENT RESULTS: During JWID 2004, C-IA COP received a warfighter and interoperability assessment.

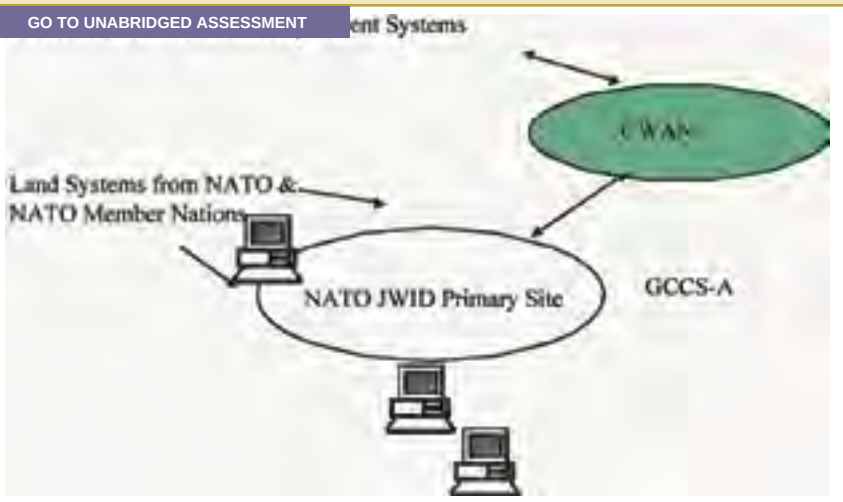
- C-IA COP successfully enhanced situational awareness in a multinational environment by linking information structure status as it related to mission critical tasks and providing computer network defense data for coalition sharing.
- The trial successfully demonstrated ability to display network readiness information and its impact on mission status while gathering information from multiple national domains for consolidated display.

CIT02.03

Global Command and Control System - Army Interoperability

GCCS-A brought an updated GCCS 4.0 to coalition JWID sites for trials. GCCS-Joint 4.0 (GCCS-J 4.0) incorporated many lessons learned from previous JWIDs, as well as new functionality to facilitate multi-security level Common Operational Picture (COP) data sharing. Loop-prevention capabilities and enhanced link data encoding permitted additional data link format exchange. Releasibility notation was also added to track encoding, providing a means for U.S. and coalition COP participants to individually mark tracks for release to any configurable operational domain.

GO TO UNABRIDGED ASSESSMENT



SPONSOR: NATO
TRIAL LOCATION: United Kingdom, NATO
TRIAL PARTNERS: N/A
OBJECTIVES: Situational awareness, database fusion and ISR dissemination

ASSESSMENT RESULTS: During JWID 2004, GCCS-A received a SEIWG evaluation report.

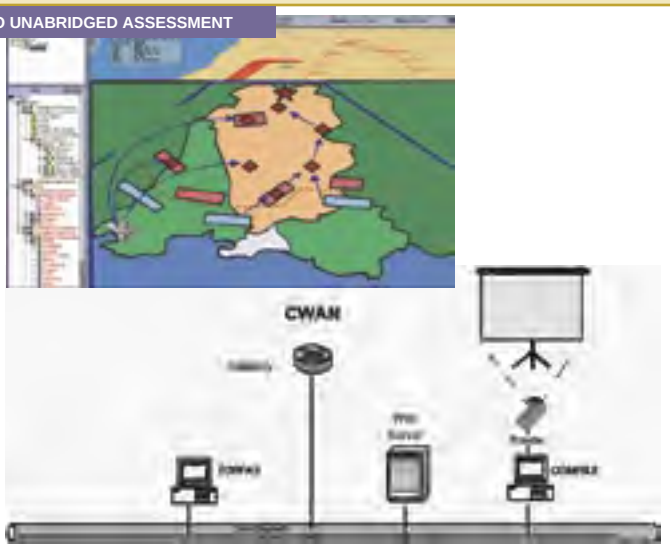
- GCCS-A successfully met all stated JWID objectives.
- It successfully forwarded tracks to LC2IS and accepted J unit feed from ICCS-A to provide a fused ground picture.
- GCCS-A provided improved situational awareness while connecting to the COP architecture via COP synchronization tool.
- The trial focused on messaging improvements by refining TADIL J - Link 16 decoding to facilitate full data interoperability on both sides of the interface. It accommodated new v4.0 data types in interoperable formats, and added AdatP-3 Baseline 11 capability.

CIT02.08

COMParison and Awareness of Situations

COMParison and Awareness of Situations (COMPASS) provided situational awareness based on comparison of the current operational situation against planned situations and tasks.

GO TO UNABRIDGED ASSESSMENT



SPONSOR: France
TRIAL LOCATION: NSWC Dahlgren; SPAWAR; NATO
TRIAL PARTNERS: CIT04.08
OBJECTIVES: Situational awareness

ASSESSMENT RESULTS: During JWID 2004, COMPASS received an interoperability assessment.

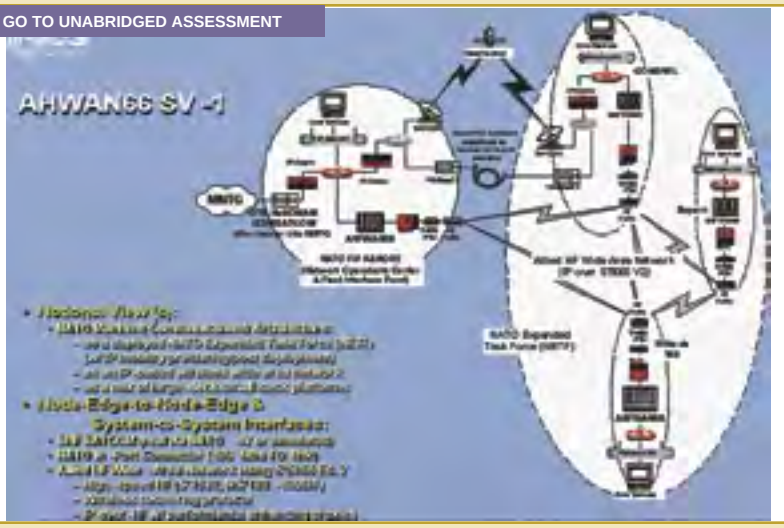
- The trial successfully met the stated JWID objective by facilitating an open portal that allowed viewing of published products derived from other individual system's data inputs.

CIT02.10

Allied HF Wide Area Network using STANAG 5006 Ed. 2

AHFWAN66 demonstrated the capabilities of High-Frequency (HF) radio as a low-cost viable remote WAN access medium for small deployed mobile networks. Utilizing modern HF radios and automated data-processing protocols, AHFWAN66 increased the reliability of HF radio networks. Additionally, AHFWAN66 demonstrated modern HF IP network's ability to provide a viable low-end access medium for military wireless WAN through increased HF transmission capacity, reduced offered traffic, and HF subnet admission control.

GO TO UNABRIDGED ASSESSMENT



SPONSOR: NATO ACT
TRIAL LOCATION: MNTG SPAWAR; MNTG NATO
TRIAL PARTNERS: CIT01.08
OBJECTIVES: Information sharing/multi-level security, situational awareness, database fusion and ISR dissemination

ASSESSMENT RESULTS: During JWID 2004, AHFWAN66 received an interoperability assessment.

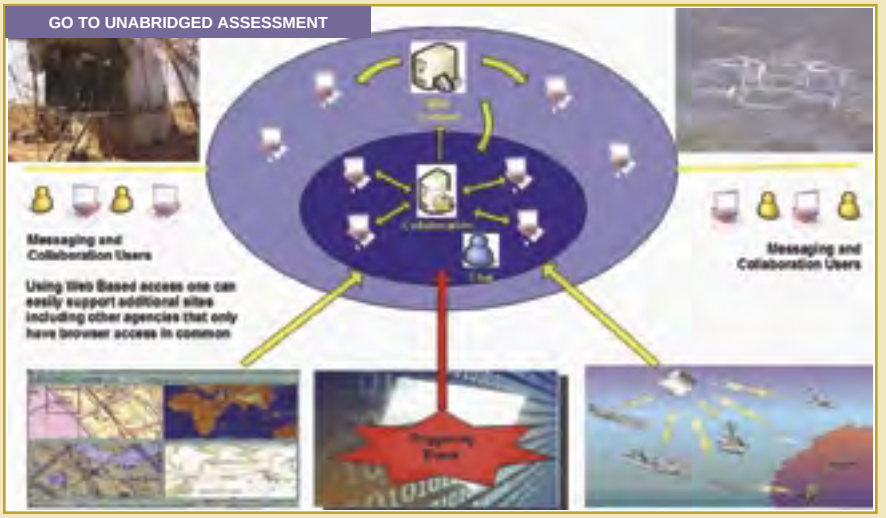
- AHFWAN66 successfully met all stated JWID objectives.
- It provided a capability for database replication/fusion and ISR Dissemination over low-bandwidth/high-latency bearer service as an integral part of a full-spectrum coalition network.
- The trial provided a capability for affordable participation in a multinational /multiple-security domain coalition network through provision of a capable Allied HF WAN.

CIT02.12

Collaboration and Messaging Demonstrator

Collaboration and Messaging Demonstrator provided Microsoft's current commercial software products to facilitate real time communication and information sharing across the coalition community. Secure access was managed by Microsoft's Active Directory for authentication and authorization to intelligence material. E-mail services included formal Military Messaging which was built for use with the Microsoft e-mail products which incremented the commercial e-mail capabilities to a "high grade" military messaging system.

GO TO UNABRIDGED ASSESSMENT



SPONSOR: Australia
TRIAL LOCATION: NSWC Dahlgren; Australia; Canada; United Kingdom
TRIAL PARTNERS: N/A
OBJECTIVES: Situational awareness and database fusion

ASSESSMENT RESULTS: During JWID 2004, Collaboration and Messaging Demonstrator received a warfighter and interoperability assessment.

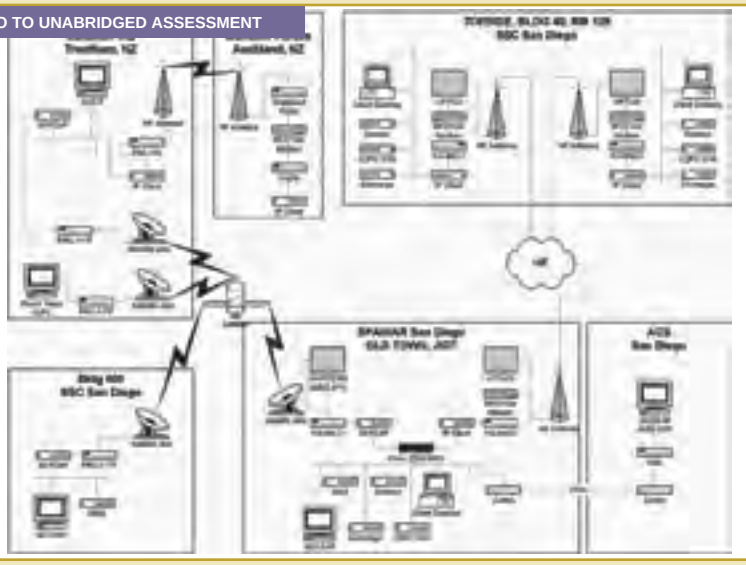
- Collaboration and Messaging Demonstrator successfully met stated JWID objectives.
- It provided improved situational awareness through standard e-mail, formal messaging, document collaboration, messaging and chat technologies.
- Warfighters considered the formal military messaging system demonstrated within the trial to be an easier product to use compared to their current formal messaging systems.

CIT02.14

SKYCAP

SKYCAP was designed as a software data control solution to provide netted IP access over half duplex low data rate satellite and terrestrial RF links. SKYCAP integrated the proposed MIL-STD-188-184A with an IP interface. The goal was to provide assured IP connectivity for COP, mail, web browsing, FTP, chat and other network functions. The demonstration showcased the STANAG 5066 HFIP suite that provides similar capabilities over HF/UHF terrestrial links. Both products are related efforts, have common software modules and integrate well together.

GO TO UNABRIDGED ASSESSMENT



SPONSOR: US Navy
TRIAL LOCATION: SPAWAR; New Zealand
TRIAL PARTNERS: N/A
OBJECTIVES: Situational awareness and ISR dissemination

ASSESSMENT RESULTS: During JWID 2004, SKYCAP received an interoperability and security assessment.

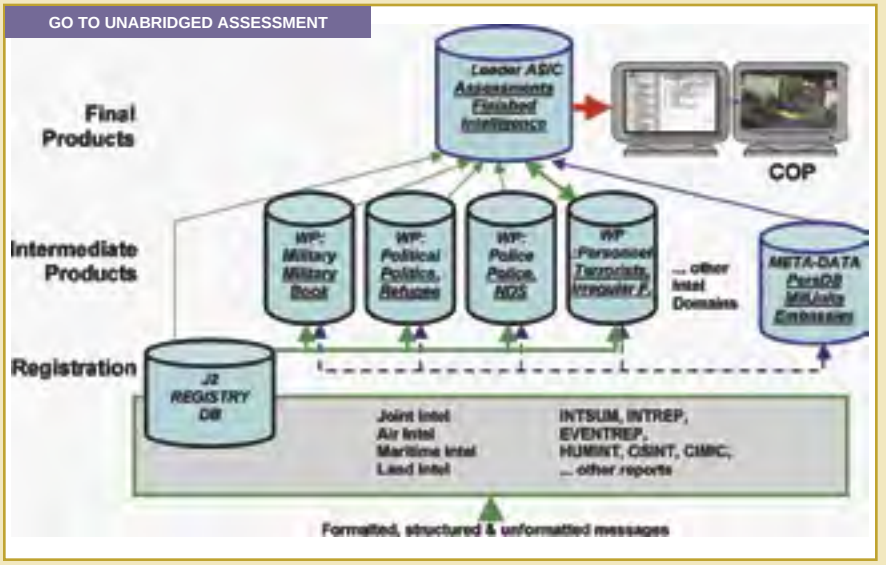
- SKYCAP successfully met stated JWID objectives while demonstrating the SKYCAP SATCOM and HFIP assured IP software suites at SPAWAR. The SKYCAP SATCOM demonstration in New Zealand was cancelled due to older firmware on the New Zealand PRCs.
- It demonstrated the capability to perform as RF extensions of the wired LAN for all types of IP based traffic.
- The trial passed standard USMTF/OTHG text messages via the GCCS NETWORK/ NETPREC interfaces to a remote node, C2PC traffic as an extension of the GCCS track picture, imagery files, chat and web browsing.

CIT02.16

German Multinational Intelligence Center

MNIC provided a local network to enhance the work of intelligence centers through improved information gathering, data fusion, and ISR dissemination. The trial provided integrated services and supported collaborative work at Military Intelligence Centers while focusing on J2 functional services for homeland security and counterterrorism. MNIC consolidated, formatted and unformatted documents and reports from various sources and produced “finished intelligence” products based on automated and interactive investigation processes.

GO TO UNABRIDGED ASSESSMENT



SPONSOR: US Navy
TRIAL LOCATION: NSWC Dahlgren; SPAWAR; NATO
TRIAL PARTNERS: N/A
OBJECTIVES: Situational awareness, database fusion and ISR dissemination

ASSESSMENT RESULTS: During JWID 2004, MNIC received a warfighter and interoperability assessments.

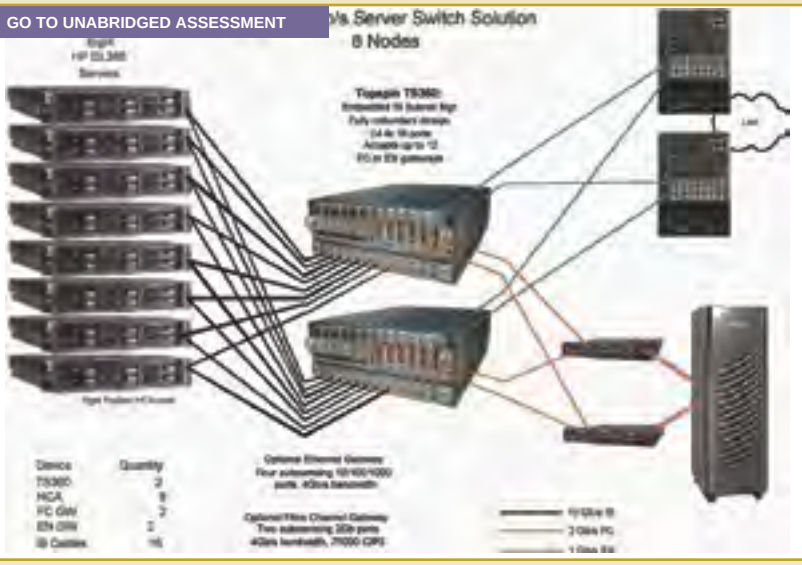
- MNIC successfully met stated JWID objectives.
- MNIC was the only JWID participating technology that successfully fused intelligence data from other JWID sources and presented a composite situational picture for planning, crisis response situations and post operations analysis.
- MNIC incorporated human intelligence through an optimized human machine interface. It effectively sifted through material and analyzed and combined raw data to produce new intelligence summaries and assessments within short reaction times in text or graphical format.

CIT02.17

Topspin

The Topspin Switched Computing System enabled industry-standard server, storage and networking resources to be rapidly deployed (and re-deployed) on-demand to match the dynamic needs of military applications. Topspin provided the ability to automatically add, remove, or shift CPU, storage, or networking horsepower from one application to another and achieve the performance of "big server iron" for as little as one tenth the costs while providing scalability for high performance computing and clustered database applications.

GO TO UNABRIDGED ASSESSMENT



SPONSOR: US Navy
TRIAL LOCATION: SPAWAR
TRIAL PARTNERS: N/A
OBJECTIVES: Situational awareness and ISR dissemination

ASSESSMENT RESULTS: During JWID 2004, Topspin received a warfighter assessment and SEIWG evaluation report.

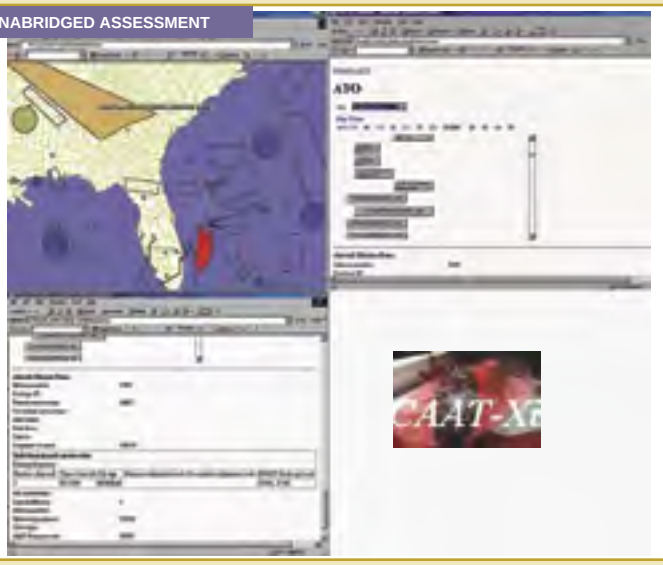
- Topspin successfully demonstrated the ability to enhance situational awareness by displaying the system status of each individual server attached to the system and the capability to send e-mail notifications in the event of a system failure.
- While Topspin did not provide ISR Dissemination tools as planned, it did indeed provide a robust environment for such tools to operate.
- The trial drew interest from SPAWAR and the Navy for its failover capabilities and situational awareness tools.

CIT02.18

Canadian ATO/ACO XML Interpreter

CAAT-Xi provided the capability to read and display the ATO and ACO in a user-friendly tabular and graphical format. CAAT-Xi was designed as a "light" application capable of importing XML formatted ATOs and ACOs, parsing the mission details and presenting the linked information in a graphical and tabular format. Additionally, it provided a mapping capability to display effective AORs, ACM types, airports, cities and target locations.

GO TO UNABRIDGED ASSESSMENT



SPONSOR: Canada
TRIAL LOCATION: NSWC Dahlgren; MNTG SPAWAR; ESC Hanscom; Australia; Canada; New Zealand; United Kingdom; NATO
TRIAL PARTNERS: CIT04.05
OBJECTIVES: Situational awareness

ASSESSMENT RESULTS: During JWID 2004, CAAT-Xi received a warfighter and interoperability assessment.

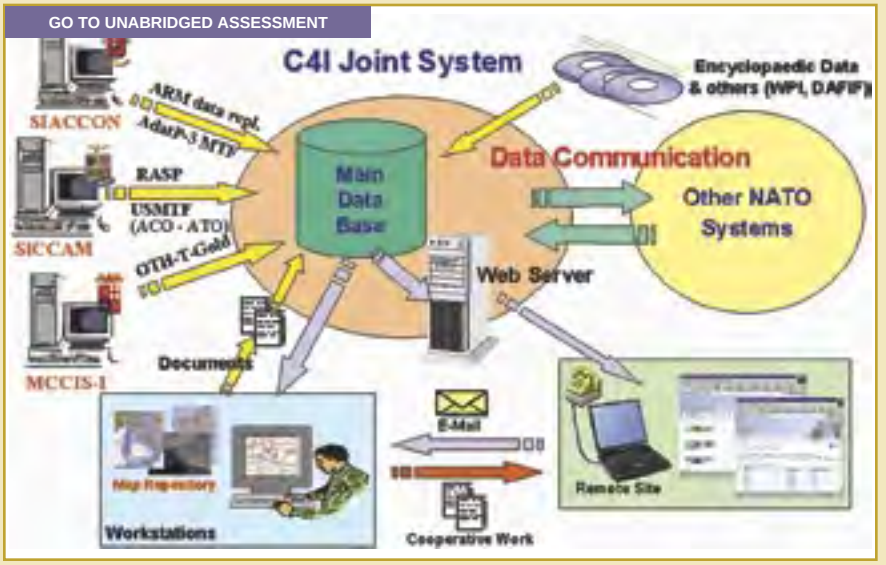
- CAAT-Xi was successful in accurately displaying information from the TBMCS generated (USMTF 2000) ATO/ACOs but display of the NATO-generated (ADatP3) ACO/ATO was not accomplished.
- CAAT-Xi was unable to fully provide its intended situational awareness for joint operations and non-air environments at the theatre level due to an operating system conflict, limited detailed ATO/ACOs used in the event, and personnel issues.

CIT02.24

C4I Difesa

The Italian C4I Joint System was designed to provide top-level strategic capabilities, lying above tactical functionalities offered by the command and control (C2) systems of each Armed Force. This trial was also designed to test data interchange between the systems of NATO/pfp, Joint and single service C2 Systems. The trial aimed to demonstrate support of high level C2 capability, Common Operational Picture (COP) interchange and situational awareness (providing COP by Web and client server applications).

GO TO UNABRIDGED ASSESSMENT



SPONSOR: Italy
TRIAL LOCATION: NATO
TRIAL PARTNERS: N/A
OBJECTIVES: Situational awareness, database fusion and fused logistics systems

ASSESSMENT RESULTS: During JWID 2004, C4I received an interoperability assessment.

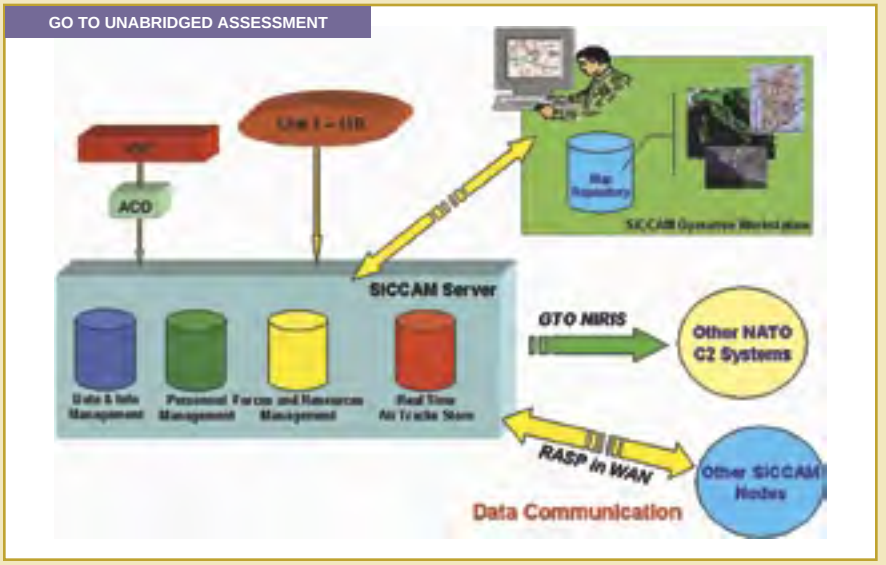
- C4I Difesa successfully met stated JWID objectives by exchanging formatted messages in various standard (GTF, ADatP-3, OTH Gold, USMTF 2000) and by data replication mechanisms while providing them to the COP.

CIT02.25

Sistema Automatizzato di Commando e Controllo

SIACCON Army C2 system was designed to be used at a tactical level, to support commanders with analysis of tactical situations, mission planning, orders and directives handling and operations monitoring. The trial was additionally designed to test data interchange between the NATO/pfp, Joint and single service C2 Systems.

GO TO UNABRIDGED ASSESSMENT



SPONSOR: Italy
TRIAL LOCATION: NATO
TRIAL PARTNERS: CIT04.03, CIT04.06
OBJECTIVES: Situation awareness

ASSESSMENT RESULTS: During JWID 2004, SIACCON received an interoperability evaluation report.

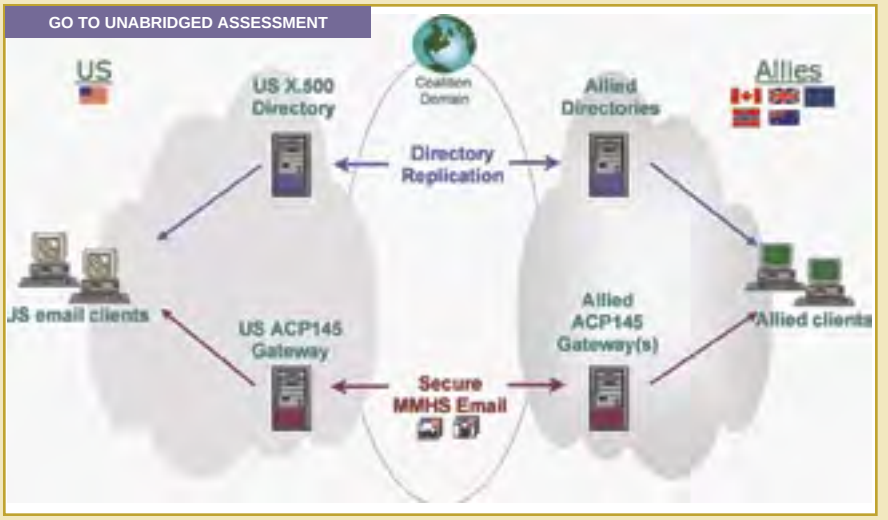
- SIACCON successfully enhanced the warfighter's situational awareness by using stored formatted intelligence messages to automatically generate AdatP3 messages to update the COP.

CIT03.03

Directory Service and Defense Military Messaging

Directory Services and DMS provided a unified view of all JWID directory information across multiple security domains to enable secure messaging between U.S. Homeland Defense and Coalition partners. The Defense Message System utilized emerging technologies to meet DoD requirements for secure, accountable, writer-to-reader messaging. The U.S. extended these capabilities to achieve messaging interoperability with Allies. These trials enabled exchange of secure X.400 military messages with Allies in a coalition environment via an ACP145 gateway.

GO TO UNABRIDGED ASSESSMENT



SPONSOR: DISA
TRIAL LOCATION: NSWC Dahlgren
TRIAL PARTNERS: N/A
OBJECTIVES: Information sharing/multi-level security and database fusion

ASSESSMENT RESULTS: During JWID 2004, DMS received SEIWG evaluation report.

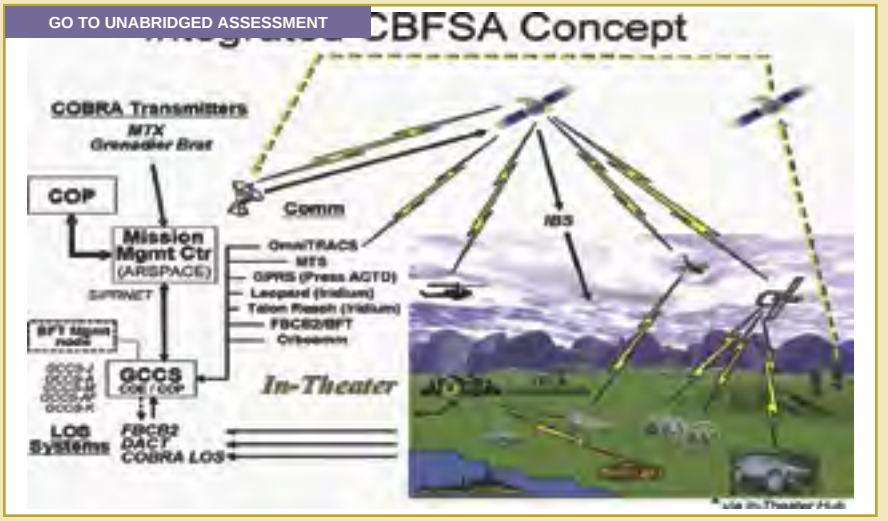
- DMS successfully met stated JWID objectives.
- Using X.500 directory replication methods, DMS successfully shared dissimilar data and presented consolidated views to the warfighter.
- The ACP145 Gateway successfully provided secure military messaging with security label processing to enable the US and Allies to migrate from the Automatic Digital Network (AUTODIN).

CIT03.04

Coalition Blue Force Situational Awareness

CBFSA provided JWID with near-real time GPS precision tracking of Friendly, Coalition and Civil Authority Forces. The primary objective was to provide a multi-unit integrated operating picture for U.S. and Coalition partners. CBFSA transmitted tracks from various BFT data devices to the Blue Force Situational awareness Mission Management Center, populated and displayed BFT data on JWID Coalition TOP COP, transferred BFT data from CFBL to NATO-unique COPs, and transferred and populated BFT data to selected Federal, State and Local Operational Centers.

GO TO UNABRIDGED ASSESSMENT



SPONSOR: USSTRATCOM
TRIAL LOCATION: USNORTHCOM; NSWC Dahlgren; SPAWAR; NATO
TRIAL PARTNERS: CIT01.01
OBJECTIVES: Information sharing/multi-level security, situational awareness, database fusion and ISR dissemination

ASSESSMENT RESULTS: During JWID 2004, CBFSA received a warfighter and interoperability assessment.

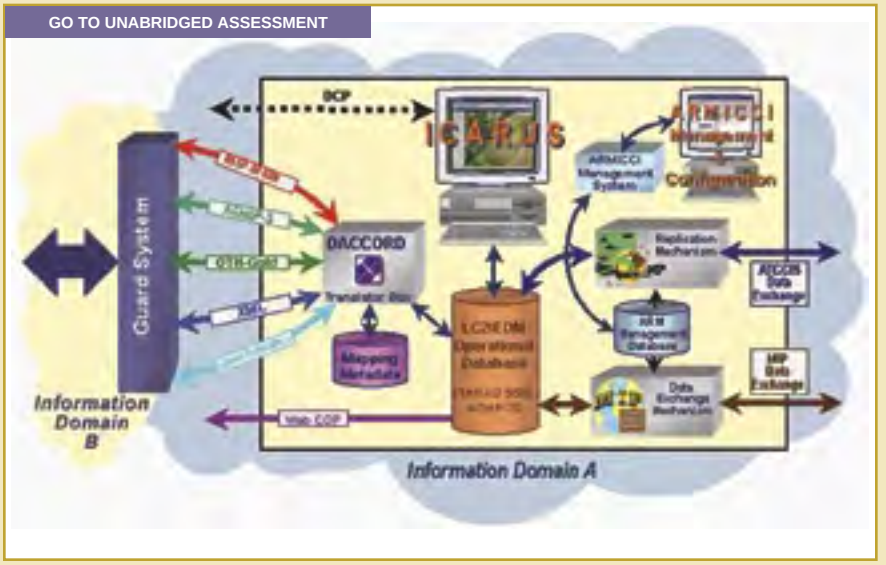
- CBFSA successfully met stated JWID objectives.
- It provided an integrated systems approach to fuse data from various devices and display the data via coalition /NATO Common Operational Picture (COP).
- The trial utilized Iridium devices to permit enhanced sharing/dissemination of ground troop locations within and across coalition systems.

CIT03.05

Incident Control and Reporting Utility System

ICARUS was designed to offer multi-functional interoperability across information domains with capabilities including DB replication message exchange and data translation functions. A mail guard solution allowed information exchange across security boundaries. Information integration through data exchange between heterogeneous systems used the configurable data translation/conversion tool DACCORD.

GO TO UNABRIDGED ASSESSMENT



SPONSOR: Germany, NATO
TRIAL LOCATION: NSWC Dahlgren; New Zealand; United Kingdom; NATO
TRIAL PARTNERS: CIT02.16
OBJECTIVES: Information sharing/multi-level security, situational awareness and database fusion

ASSESSMENT RESULTS: During JWID 2004, ICARUS received a warfighter and interoperability assessment and a SEIWG evaluation report.

- ICARUS was moderately successful in demonstrating an enhanced method to fuse and protect information contained in dissimilar databases using MIP DEM between the heterogeneous C2 system. ICARUS was successful providing data via MIP DEM to the UK C2 system, but the demonstration with Canada did not occur due to network problems. No replication connection could be established between ICARUS and the Canadian C2 system.

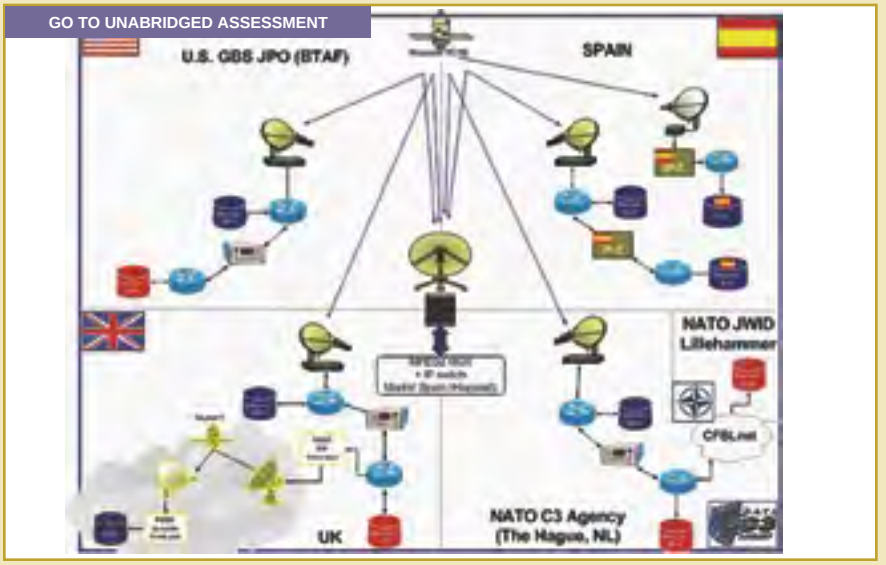
- Exchange of data with the U.S. and NZ was not accomplished. The formatted message type sent to the U.S. could not be interpreted by the system and no e-mail communication was established with users in NZ, which pro-

CIT04.02

Satellite Coalition Broadcast Environment

SCoBE implemented a two-way interoperable coalition SATCOM architecture to share information products such as streaming broadband video, high resolution imagery, and Air Tasking Orders. SCoBE was designed to enable deployed coalition forces to communicate in both directions over coalition partner satellite broadcasts and eliminate reliance on terrestrial network connectivity for dissemination of real-time tactical and reconnaissance information products.

GO TO UNABRIDGED ASSESSMENT



SPONSOR: USAF
TRIAL LOCATION: DISA Eagle; NGA; United Kingdom; NATO
TRIAL PARTNERS: N/A
OBJECTIVES: Database fusion and ISR dissemination

ASSESSMENT RESULTS: During JWID 2004, SCoBE received a warfighter assessment and a SEIWG evaluation report.

- SCoBE successfully met stated JWID objectives by providing enhanced ISR product sharing/dissemination within and across coalition systems through a digital video broadcast-return channel satellite (DVB-RCS).

- SCoBE successfully provided enhanced interoperable situational awareness by providing warfighters real-time mission related video feeds, intelligence clips and maps to accomplish assigned tasking.

- The trial's non-dependence upon LAN lines is a true plus, providing the benefit of real-time awareness in a secure environment.

CIT04.03

The Globe Suite of Tools

The Globe Suite of Tools was designed to provide analysts, commanders, warfighters and first responders with a single visualization interface that supports fusion of data from multiple GIS database sources. The suite featured advanced visualization and data interaction techniques including Black Coral GIS, a net-centric C4ISR application that provided a consolidated view of information from various stove-pipe applications, open standards-based information from world-wide agencies, and other geospatial data.

GO TO UNABRIDGED ASSESSMENT

SPONSOR: Canada
TRIAL LOCATION: USNORTHCOM; NSWC Dahlgren; SPAWAR; ESC Hanscom; NGA; Australia; Canada; United Kingdom
TRIAL PARTNERS: CIT04.04, CIT04.06, CIT01.10, CIT04.08
OBJECTIVES: Database fusion and ISR dissemination

ASSESSMENT RESULTS: During JWID 2004, The Globe Suite of Tools received a warfighter assessment and SEIWG evaluation report.

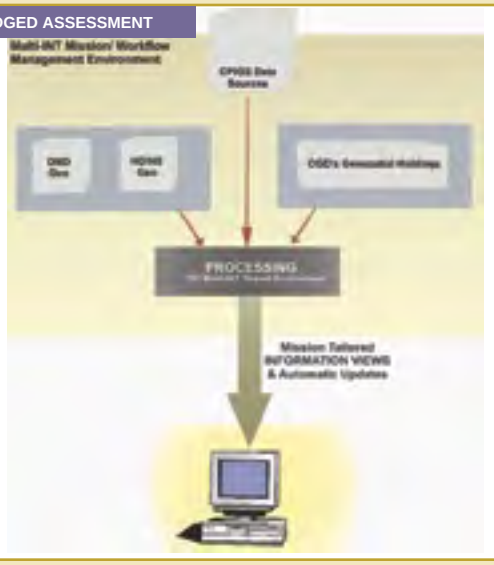
- The Global Suite of Tools successfully met stated JWID objectives by permitting access and visualization of imagery and geospatial intelligence from multiple GIS databases.
- Warfighters generally concurred the CIT worked well during JWID. Overall The Globe Suite of Tools provided value-added to perform JWID tasks. The trial provided advanced visualization capabilities not yet available commercially or to the military.

CIT04.04

Geospatial Intelligence Integration

Using Natural Resources national map as its basis, the GII effort aimed at combining all Mapping and Charting Establishment (MCE) commercial imagery, commercial geospatial data and Geospatial Intelligence products into a single, integrated database to enable key players in the Defense, Intelligence, Homeland Security Communities and the Federal Government, to fulfill their Homeland Security missions. The end result was to help resolve interoperability issues arising from cross border (U.S./CAN) datasets collected using different criteria.

GO TO UNABRIDGED ASSESSMENT



SPONSOR: Canada
TRIAL LOCATION: Canada
TRIAL PARTNERS: N/A
OBJECTIVES: ISR dissemination

ASSESSMENT RESULTS: During JWID 2004, GII received a warfighter assessment and SEIWG evaluation report.

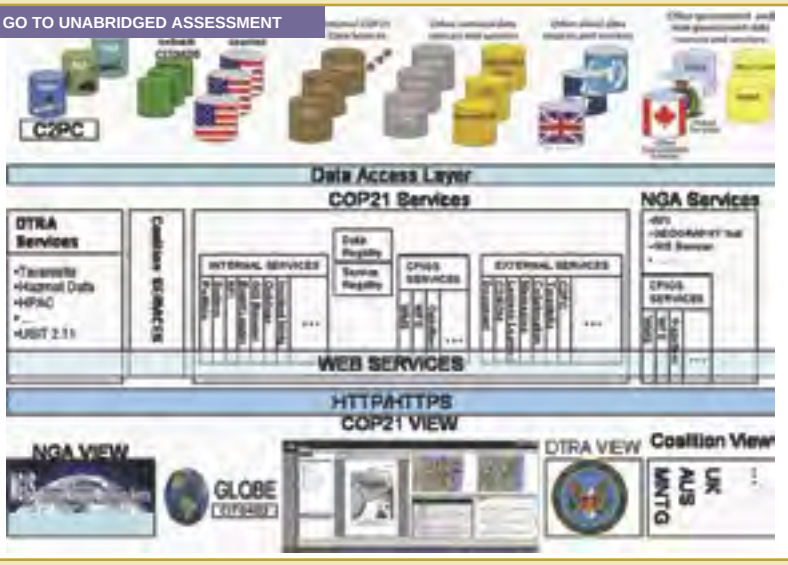
- GII successfully met the stated JWID objective.
- The GII trial highlighted incompatibilities between Canada and US data. It served primarily to identify the requirements for the development of standard operating procedures for sharing coalition mapping data.

CIT04.05

Portal to Portal Interoperability Trial

The Portal to Portal Interoperability trial was designed to investigate portal designs (primarily the COP 21 portal), examine engineering issues sharing and integrating web services and applets from different portal environments and evaluate performance and scalability issues. Additionally the trial evaluated overall situational awareness provided by the portals and integrated services, such as CPIGS, GIS browser, RFI manager, the Incident Management System, advanced search engines, and visualization services.

GO TO UNABRIDGED ASSESSMENT



SPONSOR: Canada
TRIAL LOCATION: USNORTHCOM; NSWC Dahlgren; SPAWAR; ESC Hanscom; Australia; Canada; New Zealand; United Kingdom
TRIAL PARTNERS: CIT04.03, CIT04.08
OBJECTIVES: Database fusion and ISR dissemination

ASSESSMENT RESULTS: During JWID 2004, Portal to Portal Interoperability received a warfighter and interoperability assessment.

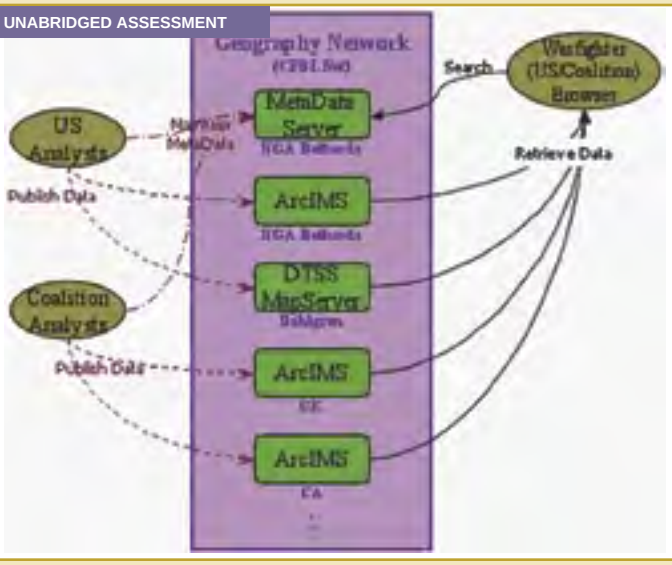
- Portal to Portal Interoperability successfully demonstrated stated JWID objectives.
- Established portfolios were shared by multiple sites using existing Geospatial Intelligence Services.
- The visualization portion of the trial was moderately successful demonstrating the fusing of information from various data sources into a homogenized view of the situation.

CIT04.06

Commercial Joint Mapping Toolkit

CJMTK provided developers of mission applications with a single, scalable, multi-tier, architecture toolkit using open development environments incorporating IT and geospatial industry standards. Using a standard architectural approach and common software components to promote interoperability, it provided the building blocks for future net-centric enterprise services as well as the legacy COE system-of-systems.

GO TO UNABRIDGED ASSESSMENT



SPONSOR: NGA, US Army
TRIAL LOCATION: NSWC Dahlgren; Australia; Canada; New Zealand; NATO
TRIAL PARTNERS: CIT04.03
OBJECTIVES: ISR dissemination

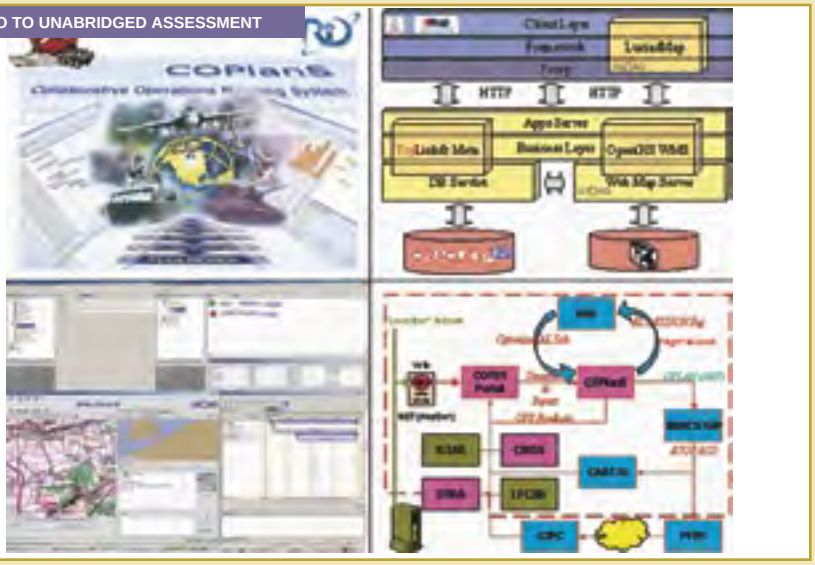
ASSESSMENT RESULTS: During JWID 2004, CJMTK received a warfighter and interoperability assessment.

- CJMTK successfully demonstrated the stated JWID objective by providing enhanced sharing/dissemination of imagery and geospatial products within and across coalition systems. It utilized the CJTMK metaserver to search and retrieve products.
- CJMTK successfully provided enhanced terrain analysis and topographic product creation through the Digital Topographic Support System (DTSS).

CIT04.08
Collaborative Operations Planning System

COPlanS was designed to provide a net centric environment through an integrated flexible suite of planning, decision-aid and workflow management tools aimed at supporting a distributed team. Offering functions to design and manage multiple concurrent distributed battle rhythms at different planning levels, it helped synchronize work flows, document processes and replay the decision-making path. COPlanS provided planning tools and decision aid tools to support the Commander's decision making process.

GO TO UNABRIDGED ASSESSMENT



SPONSOR: Canada
TRIAL LOCATION: ESC Hanscom; Australia; Canada; New Zealand; United Kingdom
TRIAL PARTNERS: CIT01.08
OBJECTIVES: ISR dissemination

ASSESSMENT RESULTS: During JWID 2004, CJMTK received a warfighter and interoperability assessment.

- COPlanS successfully demonstrated stated JWID objectives by sharing Microsoft Office products, graphic files, and PDF files between users. This information sharing helped improve the staff's course of action assessment that was distributed to all users.
- Due to its chronological structure, COPlanS helped improve decision making as it walked users through the entire planning process.

CIT04.09
Enterprise Knowledge Management

eKM supported JWID as the CTF staff web services tool with a centralized storage repository, secure socket layer encryption technology with user name and password protection, NIPRNET and SIPRNET availability, customizable memberships in COPs, and e-mail connectivity. The system was capable of capturing and managing information while providing storage for public or private sharing, managing business processes, organizing web sites, tracking leave, and permitting ad hoc searches on keywords, authors, editors, and applications.

GO TO UNABRIDGED ASSESSMENT

SPONSOR: US Navy
TRIAL LOCATION: NSWC Dahlgren
TRIAL PARTNERS: N/A
OBJECTIVES: ISR dissemination

ASSESSMENT RESULTS: During JWID 2004, eKM received a warfighter and security assessment and a SEIWG evaluation report.

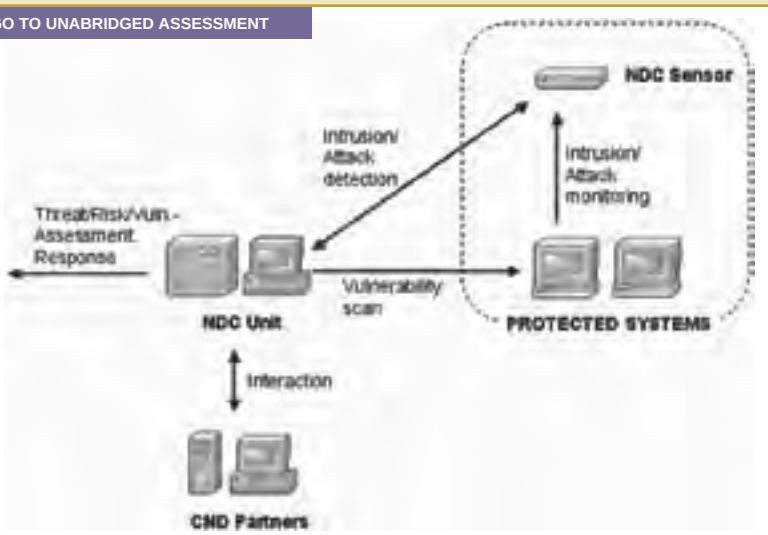
- eKM successfully demonstrated stated JWID objectives by sharing and disseminating information among nations using coalition networks with a web-based collaboration environment and document workflow capabilities.
- eKM enabled the Coalition Task Force to access all pertinent documents in one location employing an easy to use search engine.
- Warfighters collectively agreed that eKm was an invaluable tool that provided a powerful means for knowledge management.

CIT06.01

Norwegian Defence Computer Network Operations Unit

The NDC Unit was comprised of technical equipment, personnel and procedures for executing computer network operations. The NDC Unit concentrated on concept development and experimentation (CDE) for monitoring and protecting information domains. The trial's primary area of interest was exchanging attack and vulnerability information. Using a wide range of sensors, the NDC Unit aggregated and correlated data to provide security information awareness for the protected system.

GO TO UNABRIDGED ASSESSMENT



SPONSOR: Norway
TRIAL LOCATION: NSWC Dahlgren; NATO
TRIAL PARTNERS: N/A
OBJECTIVES: Coalition network defense

ASSESSMENT RESULTS: During JWID 2004, NDC Unit was scheduled to receive a warfighter and interoperability assessment.

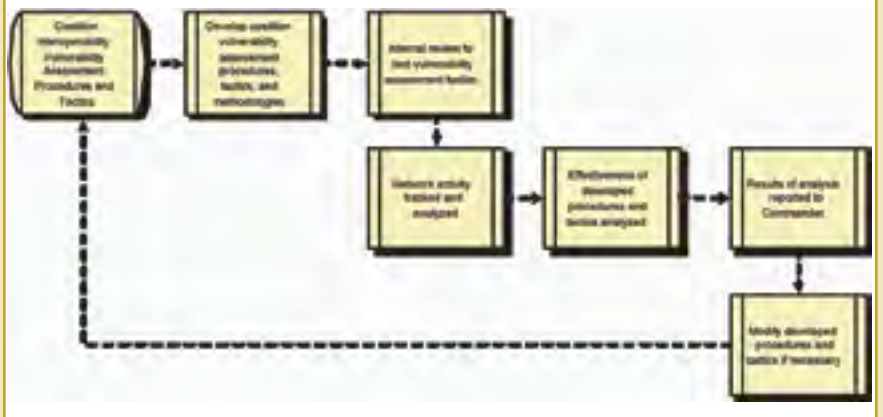
- The NDC Unit successfully demonstrated stated JWID objective by defending the Norwegian network and systems from any unauthorized attacks.
- During JWID execution the NDC Unit performed exceptionally well collecting computer network attack data, formulating courses of action, and coordinating and directing mission-critical solutions.
- The U.S. interoperability assessment did not occur because there was no data exchange with U.S. systems and the required data interfaces could not be implemented. Data exchanges observed at NATO were carried out with human intervention, but were a first step in automated system to system communication.

CIT06.04

Coalition Interoperability Vulnerability Assessment Procedures and Tactics

CIVAPT developed procedures, methodologies, and tactics to conduct vulnerability assessments to defend coalition networks from Cyber-threats. CIVAPT's intent was to provide solutions for enhanced sharing/ dissemination of intelligence and surveillance across coalition/interagency domains by testing developed tactics, techniques, and procedures for use of network protection, detection, and reaction technologies. The results were to provide insight on cyber risks associated with computers, systems and networks used in decision-making.

GO TO UNABRIDGED ASSESSMENT



SPONSOR: DISA
TRIAL LOCATION: NSWC Dahlgren
TRIAL PARTNERS: CIT01.25, CIT04.09, CIT01.09
OBJECTIVES: ISR dissemination and coalition network defense

ASSESSMENT RESULTS: During JWID 2004, CIVAPT was scheduled to receive a warfighter assessment and SEIWG evaluation report.

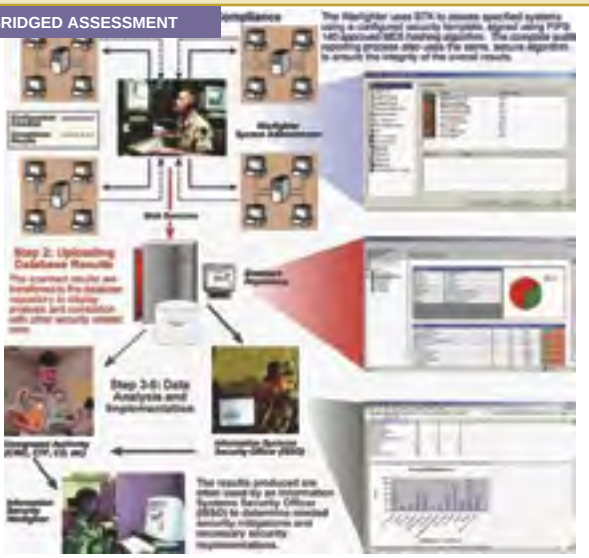
- Due to network security constraints, CIVAPT was not capable of demonstrating detection of network vulnerabilities stemming from "insider" abuses.
- CIVAPT was also unable to test procedures, methodologies, and tactics to allow interoperability while conducting vulnerability assessments to defend networks from cyber-threats.
- Although a warfighter assessment was planned for CIVAPT, and questionnaires were assigned to two warfighters, no pertinent data was retrieved to permit a viable assessment.

CIT06.05

Baseline Toolkit

BTK was designed as a field deployable application to access security related data from computers operating on Microsoft® Windows NT 4.0 or Windows 2000 domains. It was designed to identify vulnerabilities on a computer, domain, or entire network. Analyzing data against configuration checklists, BTK could deliver collected data in an easy to read XML file. BTK also provided ability to scan computers to identify systems on a domain that did not meet baseline security requirements and to ensure Information Assurance Vulnerability Alert (IAVA) compliance.

GO TO UNABRIDGED ASSESSMENT



SPONSOR: USMC
TRIAL LOCATION: NSWC Dahlgren; SPAWAR; Australia; Canada; United Kingdom
TRIAL PARTNERS: N/A
OBJECTIVES: Situational awareness, ISR dissemination and coalition network defense

ASSESSMENT RESULTS: During JWID 2004, BTK received a warfighter and security assessment.

- BTK successfully demonstrated ability to monitor and defend computers and computer systems/networks by creating baseline security checklists for computer security. It allowed warfighters to initiate and conduct security and vulnerability scans and retrieve security posture results.

- BTK also demonstrated ability to eradicate any system discrepancies with minimal or no impact to the ongoing mission.